République Tunisienne
Ministère des Technologies de la Communication

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

SECURITE INFORMATIQUE

GLOSSAIRE de la

Cryptanalyse
Cryptographie
Cybersquatting (cybersquattage)
Défacement (défaçage ou Webdefacing)
Déni de service (Deny of service ou Denial of Service ou DoS)
Dépassement ou débordement de mémoire (buffer overflow)
Disponibilité d'un équipement ou d'un système
Dropper ou implanteur ou injecteur
DMZ (demilitarized zone ou zone démilitarisée)
Evènement de sécurité
Exploit (ou programme d'exploitation)
Filtrage
Firewall (pare-feu)
Flooding
Forensics
Hacker (pirate ou intrus)
Heuristique
Hijacker
Hoax (canular) Honeynet (ou Honeynet ou pot de miel)
Identification
IDS/IPS : Intrusion Detection/Prevention System
Incident
Ingénierie sociale
Intégrité
Intrusion
ISO 2700x
Investigation
Journalisation (logging)
Keylogger
Log
Logiciel de contrôle parental ou de filtrage
Malware
Menace
Méthodologie d'audit
Non répudiation
Norme de sécurité
Patch (correctif de sécurité)
PCA (Plan de continuité ou plan de continuité d'activité)
Pen testing (Test d'intrusion)
Pharming
Phishing (hameçonnage)
Phreaking
PKI (Public Key Infrastructure)
Politique de sécurité
Protocole sécurisé SSL (Secure Sockets Layer)
Protocole TLS (Transport Layer Security)
Proxy ou serveur mandataire
Réseau social
Risque
RootKit
RTO (Recovery Time Objective ou durée maximale d'interruption admise)
SI (Responsable de la sécurité des systèmes d'information ou CSSI)
Signature électronique
Scam ou arnaque
Sauvegarde
SMSI (Système de Management de la Sécurité de l'Information)
Spam
Ver (Worm)
Virus
VPN (Virtual Private Network ou réseau privé virtuel ou RPV)
Vulnérabilité ou faille
WEP (Wired Equivalent Privacy)
Wi-Fi ou Wireless Fidelity ou Ethernet sans fil
WAP (Wireless Application Protocol)
XSS (Cross Site Scripting)

tunCERT
Tunisian Computer Emergency ResponseTeam

GLOSSAIRE de la SECURITE INFORMATIQUE

Proxy ou serveur mandataire
Réseau social
Risque
RootKit
RSSI (Responsable de la sécurité des systèmes d'information ou CISO)
RTO (Recovery Time Objective ou durée maximale d'interruption admissible)
Serveur
Sauvegarde
Scam ou arnaque
Signature électronique
SMSI (Système de Management de la Sécurité de l'Information)
Sniffer
Spam
Spoofing (usurpation d'identité électronique)
Spyware (logiciel espion)
SSH (Secure Shell)
Stateful inspection (filtrage de paquets dynamique)
Switch (commutateur réseau)
TypoSquatting
Ver (Worm)
Virus
VPN (Virtual Private Network ou réseau privé virtuel ou RPV)
Vulnérabilité ou faille
WEP (Wired Equivalent Privacy)
WI-FI ou Wireless Fidelity ou Ethernet sans fil
WAP (Wireless Application Protocol)
XSS (Cross Site Scripting)

ActiveX
Adresse IP
ANSI (Agence Nationale de la Sécurité Informatique)
ANSI (American National Standards Institute)
Anti-virus
Appliance
Archivage électronique
Attaque
Audit sécurité
Authentification
Backdoor (Porte dérobée)
Backup
Biométrie
Black List (liste noire)
Bombe logique
Brute Force
Botnet (réseau Zombie)
Certificat électronique
CERT (Computer Emergency Response Team)
Cheval de Troie (troyen ou trojan horse)
Chiffrement (cryptage)
Code source
Cookie
Confidentialité
Contournement de la politique de sécurité
Contrôle d'accès
Clé
Clonage de serveur DNS (DNS pharming)
Cryptanalyse
Cryptographie
Cybersquatting (cybersquattage)
Défacement (défaçage ou Webdefacing)
Déni de service (Deny of service ou Denial of Service ou DoS)
Dépassement ou débordement de mémoire (buffer overflow)
Disponibilité d'un équipement ou d'un système
Dropper ou implanteur ou injecteur
DMZ (demilitarized zone ou zone démilitarisée)
Evènement de sécurité
Exploit (ou programme d'exploitation)
Filtrage
Firewall (pare-feu)
Flooding
Forensics
Hacker (pirate ou intrus)
Heuristique
Hijacker
Hoax (canular) Honeypot (ou Honeynet ou pot de miel)

SOMMAIRE

GLOSSAIRE de la SECURITE INFORMATIQUE

ActiveX: Technologie de Microsoft qui permet d'insérer des effets multimédias et des animations dans des pages Web. Son implémentation la plus courante est le «contrôle ActiveX», téléchargeable et exécutable par un navigateur web et permettant l'accès aux éléments d'un environnement Microsoft. Les contrôles ActiveX sont utilisés aussi bien par les sites de mise à jour (Ex celui de Microsoft Windows:http//WindowsUpdate.microsoft.com), que par des programmes malveillants.

Adresse IP: Identifiant numérique. Sur Internet/réseau, les machines (PC, Tel, Imprimante,…) sont identifiées par des adresses numériques, appelées adresses IP, qui assurent l'intercommunication à travers des protocoles spécifiques (protocole IP). L'adresse IP peut être publique ou privée. RFC 1918

ANSI: (Agence Nationale de la Sécurité Informatique) Organisme public qui veille et à la protection des systèmes informatiques et des réseaux relevant des divers organismes publics et privés.

ANSI: (American National Standards Institute) Organisme privé à but non lucratif qui supervise le développement de normes pour les produits, les services, les procédés, les systèmes et les employés des États-Unis. Ces normes sont proposées à partir d'une démarche volontaire et consensuelle.

Anti-virus: Logiciel de détection, recherche et nettoyage des programmes malicieux (virus, malware). Il utilise plusieurs méthodes, pour les identifier, les bloquer et/ou les éradiquer, telles que:

- *Méthode utilisant la base de signature virale qui contient le code numérique des virus (signature virale),*

- *Méthode heuristique en tendant à découvrir le programme malveillant par son comportement.*

Appliance: Tout système vendu comme «prêt à l'emploi». Présenté comme une boite noire sur laquelle l'applicatif est préinstallé, l'appliance n'est pas destiné à exécuter d'autres tâches que celles pour lesquelles il a été conçu (serveur Web, d'impression, de fichiers, de messagerie, etc.).

Archivage électronique: Ensemble des actions, outils et méthodes mis en oeuvre pour réunir, identifier, sélectionner, classer et conserver des contenus électroniques, sur un support sécurisé, dans le but de les exploiter et de les rendre accessibles dans le temps, que ce soit à titre de preuve (en cas d'obligations légales notamment ou de litiges) ou à titre informatif. Le contenu archivé est considéré comme figé et ne peut donc être modifié.

Attaque: Action de malveillance consistant à tenter de contourner les fonctions de sécurité d'un Système Informatique. Il existe deux types

d'attaques, les attaques passives et les attaques actives. Une attaque passive ne modifie pas le fonctionnement normal des communications et du réseau: elle se base sur l'Observation et l'Analyse du trafic. Une attaque active modifie l'état de la communication et du réseau et prend 3 formes possibles: Altération des messages, Refus de Service et Connexion frauduleuse.

Audit sécurité: Vue à un instant T de tout ou partie du SI, permettant d'évaluer le niveau de sécurité du SI par rapport à un référentiel.

L'audit répertorie les points forts, et surtout les points faibles (vulnérabilités) de tout ou partie du système. L'auditeur dresse également une série de recommandations pour supprimer les vulnérabilités découvertes. L'audit est généralement réalisé conjointement à une analyse de risques, et par rapport au référentiel.

Authentification: Identification d'un utilisateur et vérification de ses droits d'accès aux services d'un système informatique. Deux niveaux sont possibles: authentification simple utilisant une seule méthode d'identification généralement basée sur une preuve mentale (mot de passe par exemple) et authentification forte utilisant au moins deux méthodes d'identification: une preuve mentale et une preuve dynamique (carte à puce par exemple).

Backdoor *(Porte dérobée)***:** Programme malveillant visant à détourner les fonctionnalités d'une application ou d'un système, en ouvrant et en exploitant des ports ou des canaux d'accès (Porte dérobée). Un Backdoor est généralement mis en place à l'aide d'un cheval de Troie.

Backup: Sauvegarde de données. Il peut aussi référer à un système de redondance pour les applications vitales d'une entreprise (dans le sens de système de secours).

Biométrie: Une des méthodes d'authentification (authentification forte). Elle permet d'authentifier une personne en numérisant ses caractéristiques physiques, telles que ses empreintes, sa rétine et le son de sa voix.

Black List (liste noire): Mécanisme de contrôle d'accès qui permet à tous les internautes/utilisateurs ou aux objets (programme, logiciel,…) d'accéder à une ressource (site web,…), sauf aux membres de la liste noire. L'opposé est une liste de confiance ou white-list, qui signifie l'interdiction d'accès qu'aux membres de cette dernière.

Bombe logique: Type de virus. Il consiste en un programme indépendant dont le rôle est de relâcher dans un système, à une date donnée ou à l'occurrence d'un événement particulier, le programme de type ver (Worm) ou autre qu'il contient.

Brute Force: Méthode utilisée en cryptanalyse qui consiste principalement à expérimenter toutes les combinaisons possibles pour casser les codes d'accès.

Botnet *(réseau Zombie)*: Ordinateur contrôlé à l'insu de son utilisateur par un pirate informatique à travers le réseau/ Internet.

Certificat électronique: Fichier délivré par une autorité de certification à une entité morale (entreprise, serveur Web,…) en tant que preuve de son identité vérifiable par tout individu. Ce fichier contient la clé publique de l'entité, une information cryptée par l'autorité de certification et des informations générales de l'entité (nom, adresse,…)

CERT *(Computer Emergency Response Team)*: Centre de veille, d'alerte et de réaction aux incidents et attaques informatiques qui ciblent les systèmes d'information professionnels ou privés.

Cheval de Troie *(troyen ou trojan horse)*: Programme qui apparaît légitime alors qu'il contient un autre programme capable de générer des actions illégales. Le programme lui-même n'étant pas un virus mais un véhicule innocent utilisé souvent pour accéder frauduleusement à des ressources.

Chiffrement *(cryptage)*: Méthode cryptographique utilisée afin de coder un texte clair pour le rendre incompréhensible, par l'intermédiaire d'une clé de chiffrement (symétrique ou asymétrique) et d'un algorithme spécifique.

Code source: Ensemble d'instructions écrites dans un langage de programmation informatique de haut niveau, c'est-à-dire humainement compréhensible, permettant d'obtenir un programme compilé pour un ordinateur.

Cookie: Petit fichier, appelé aussi témoin, créé par le navigateur Web dans le disque dur et destiné à mémoriser les coordonnées des pages Web visitées, afin de pouvoir les ouvrir plus rapidement lors de la prochaine visite.

Confidentialité: Propriété cruciale associée aux données sensibles (mot de passe,…) et à certaines applications (EDI, messageries électroniques,…). Elle est généralement assurée par les techniques de cryptage.

Contournement de la politique de sécurité: Toute action ayant pour conséquence la mise en échec des règles ou des mécanismes de sécurité mis en place.

Contrôle d'accès: Le fait d'autoriser ou d'interdire aux utilisateurs l'accès à des ressources d'un système.

Clé: Chaîne de caractères utilisée par une

technique de chiffrement soit pour coder soit pour décoder des données. Une clé publique est connue de tous et est utilisée pour coder. Une clé privée n'est connue que par le concerné et est utilisée pour décoder.

Clonage de serveur DNS *(DNS pharming)***:** Activité malveillante visant à modifier un serveur DNS (serveur de noms de domaine), dans le but de rediriger un nom de domaine vers une adresse IP différente de l'adresse légitime.

Cryptanalyse: Ensemble des techniques visant à transformer à l'aide de conventions secrètes des informations ou signaux clairs en informations ou signaux inintelligibles pour des tiers, ou à réaliser l'opération inverse.

Cryptographie: Discipline incluant les principes, moyens et méthodes de transformation des données, dans le but de cacher leur contenu, d'empêcher que leur modification passe inaperçue et/ou d'empêcher leur utilisation non autorisée. ISO 7498-2

Cybersquatting (cybersquattage): Pratique consistant à enregistrer un nom de domaine correspondant à une marque, avec l'intention de le revendre ensuite à l'ayant-droit.

Défacement (défaçage ou Webdefacing): Modification non sollicitée du contenu d'une page d'un site Web.

Déni de service *(Deny of service ou Denial of Service ou DoS)* **:** Ensemble de techniques d'attaques, venant d'une même source, ayant pour but d'interrompre la fonction d'un serveur et de le rendre indisponible. La méthode la plus classique consiste à faire crouler le serveur sous une masse de requêtes généralement mal formées pour entraîner une réponse anormale et paralysante. Une attaque distribuée venant de plusieurs sources est appelée DDoS.

Dépassement ou débordement de mémoire *(buffer overflow)***:** Technique d'exploitation d'une vulnérabilité dans le code d'un programme qui ne vérifie pas correctement la taille de certaines données qu'il manipule.

Disponibilité d'un équipement ou d'un système: Propriété d'être accessible et utilisable à la demande par une entité autorisée. ISO/IEC 27001:2005

Dropper ou implanteur ou injecteur: Programme capable d'implanter un exécutable malveillant sur une machine locale.

DMZ *(demilitarized zone ou zone démilitarisée)***:** Zone qui se situe entre un réseau interne et un réseau public

qui permet d'isoler certains serveurs de l'entreprise à usage public (serveurs Web, FTP, etc.), généralement contrôlée par un Firewall.

Evènement de sécurité: Occurrence identifiée d'un état d'un système, d'un service ou d'un réseau, indiquant une brèche possible dans la politique de sécurité du système de l'information ou un échec des moyens de protection, ou encore une situation inconnue jusqu'alors et pouvant relever de la sécurité. ISO/IEC 27001:2005

Exploit *(ou programme d'exploitation)***:** Programme permettant de se servir d'une faille (vulnérabilité) pour pirater, modifier ou détourner un système ou un logiciel de son fonctionnement normal. Exploit est souvent employé comme synonyme de Proof of concept (ou PoC: démonstration de faisabilité). Un exploit peut éventuellement être utilisé à des fins malveillantes alors qu'un PoC ne l'est pas.

Filtrage: Technique de contrôle de flux sur un réseau qui empêche le passage des informations jugées suspectes. On distingue 3 niveaux de filtrage: filtrage IP (assuré généralement par un routeur), filtrage de contexte (relatif à l'état des connexions) et filtrage applicatif (assuré généralement par un proxy).

Firewall *(pare-feu)***:** Elément du réseau informatique, logiciel et/ou matériel, qui a pour fonction de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communication autorisés ou interdits.

Flooding: Technique d'attaque par déni de service qui consiste à envoyer un grand nombre de requêtes simultanées vers une machine pour entraîner sa défaillance.

Forensics: Ensemble des techniques utilisées pour les recherches effectuées sur une machine suite à une intrusion et cela afin d'en isoler les causes et les conséquences.

Hacker *(pirate ou intrus)***:** Personne ayant une bonne connaissance et maîtrise de l'informatique et des réseaux. Pour éprouver son savoir, elle cherche généralement à se mesurer à des systèmes très sécurisés en s'y infiltrant, et ce, afin de les espionner ou de les endommager.

Heuristique: Méthode de détection virale s'appuyant sur des recherches d'instructions suspectes et des anomalies structurelles de fichiers laissant supposer la présence d'un code suspect.

Hijacker: Programme qui interfère avec un navigateur Internet afin de rediriger secrètement ou non son utilisateur vers un

site qu'il n'a pas choisi (modification de la page d'accueil ou de la liste des favoris, redirections trompeuses, etc.).

Hoax (canular): E-mail diffusant une fausse information, concernant principalement une alerte de propagation d'un virus virulent.

Honeypot *(ou Honeynet ou pot de miel)***:** Système leurre volontairement non sécurisé et connecté à Internet, destiné à subir des attaques qui sont ensuite collectées à des fins d'analyse.

Identification: Procédure permettant de reconnaître un utilisateur afin de lui accorder les droits correspondant à son profil.

IDS/IPS: Intrusion Detection/Prevention System: Outils destinés à détecter et alerter, voire bloquer, les activités suspectes sur la cible analysée (un réseau ou un hôte).

Incident: Evènement inattendu.

Ingénierie sociale: Technique consistant à utiliser une fausse identité ou un prétexte afin de soutirer un mot de passe, un document ou toute information confidentielle.

Intégrité: Assurance que les données n'ont pas été modifiées (par des personnes non autorisées) pendant le stockage ou la transmission.

Intrusion: Accès non autorisé à un système informatique afin de lire ses données internes ou d'utiliser ses ressources.

ISO 2700x: Famille de normes concernant la gestion de la sécurité du système d'information:

ISO 27001: norme de certification d'un SMSI.

ISO 27002: code de bonnes pratiques pour la sécurisation d'un système d'informations.

ISO 27005: gestion du risque en sécurité de l'information.

ISO 27006: exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information.

Investigation: Action de suivre à la trace, de rechercher attentivement.

Journalisation *(logging)***:** Action d'archiver des informations à propos d'événements, tels que les connexions, la gestion des fichiers ou, plus généralement, sur le trafic qui passe sur un réseau.

Keylogger: Programme qui espionne les frappes du clavier.

Log: Fichier dans lequel des événements d'un certain type sont consignés au fur et à mesure qu'ils se produisent.

Logiciel de contrôle parental ou de filtrage: Systèmes de protection qui s'installent sur un ordinateur et qui permettent notamment de bloquer l'accès aux sites inappropriés aux plus jeunes. Certains permettent également de paramétrer l'accès à l'Internet (plages horaires, durée, applications…). Tout ordinateur personnel utilisé par un mineur devrait en être équipé.

Malware: Logiciel malveillant. Les virus et les vers sont les deux exemples de logiciels malveillants les plus connus.

Menace: Cause potentielle d'un événement indésirable, pouvant entraîner des dommages au sein d'un système ou d'un organisme.

ISO/IEC 27002:2005

Méthodologie d'audit: Démarche à entreprendre pour arriver efficacement à un résultat précis.

Non répudiation: Propriété exprimant la reconnaissance d'un acte électronique (transaction, réception de données, …). Elle peut être assurée par des techniques à base de preuves.

Norme de sécurité: Document de référence basé sur un consensus couvrant un large intérêt industriel ou économique et établi par un processus volontaire. Deux variantes principales d'une norme: un standard guide (ensemble de bonnes pratiques: exemple ISO 27002) et un standard exigences (ensemble de clauses à satisfaire pour pouvoir être certifié: exemple ISO 27001).

Patch (correctif de sécurité): Programme destiné à corriger un disfonctionnement de logiciel et diffusé par l'éditeur de celui-ci.

PCA *(Plan de continuité ou plan de continuité d'activité)***:** Ensemble de mesures visant à assurer, selon divers scénarios de crise, le maintien, le cas échéant de façon temporaire selon un mode dégradé, des prestations de services essentielles de l'entreprise puis la reprise planifiée des activités.

Pen testing *(Test d'intrusion)***:** Action qui consiste à essayer plusieurs codes d'exploitation sur un système d'information, afin de déterminer ceux qui donnent des résultats positifs.

Pharming: Attaque visant à rediriger le trafic d'un site Web vers un site malicieux.

Phishing *(hameçonnage)*: Technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance - banque, administration, etc. - afin de lui soutirer des renseignements personnels: mot de passe, numéro de carte de crédit, date de naissance, etc. L'hameçonnage peut se faire par courrier électronique, par des sites web falsifiés ou autres moyens électroniques.

Phreaking: Technique de piratage consistant à téléphoner gratuitement sur de longues distances en piratant une ligne téléphonique.

PKI *(Public Key Infrastructure)*: Infrastructure de gestion de clés de cryptage.

Politique de sécurité: Règlement interne en matière de sécurité du système d'information qui doit être conforme aux règlements, obligations contractuelles, directives, normes, procédures et guides auxquels est soumise l'entreprise.

Protocole sécurisé SSL *(Secure Sockets Layer)*: Protocole établissant une liaison de communication sécurisée destinée à empêcher l'interception, sur le Web ou par d'autres services liés à Internet, d'informations à caractère critique, telles que des numéros de carte de paiement.

Protocole TLS *(Transport Layer Security)*: Protocole assurant la confidentialité et la sécurité des communications entre deux applications sur un réseau. Ce protocole permet également aux clients d'authentifier des serveurs ou, en variante, à des serveurs d'authentifier des clients.

Proxy ou serveur mandataire: Serveur informatique qui a pour fonction de relayer des requêtes entre un poste client et un serveur.

Réseau social: Ensemble d'entités sociales telles que des individus ou des organisations sociales reliées entre elles par des liens créés lors des interactions sociales. Il se représente par une structure ou une forme dynamique d'un groupement social. Il existe des applications Internet aidant à se créer un cercle d'amis, à trouver des partenaires commerciaux, un emploi ou autres.

Risque: Combinaison de la probabilité de l'occurrence d'un événement et ses conséquences. ISO/IEC 27002:2005

RootKit: Code malicieux permettant à un attaquant de maintenir, dans le temps, un accès frauduleux à un système informatique.

RSSI *(Responsable de la sécurité des systèmes d'information ou CISO)*: Responsable d'une organisation (entreprise, association ou institution) qui y est responsable du maintien du niveau de sécurité du système d'information.

RTO *(Recovery Time Objective ou durée maximale d'interruption admissible)*: Temps maximal acceptable durant lequel une ressource peut ne pas être fonctionnelle après une interruption majeure de service.

Serveur: Un des éléments participant au mode de communication client serveur entre des logiciels: un logiciel dit « client » envoie une requête à un logiciel « serveur » qui lui répond, le tout suivant un protocole de communication. Par extension, on désigne par serveur informatique l'ordinateur hébergeant de tels logiciels serveurs. Les logiciels clients s'y connectent à travers un réseau informatique. Les serveurs offrent des services qui permettent, par exemple, de stocker des fichiers, transférer le courrier électronique, héberger un site Web, etc. Il est possible pour un ordinateur ou un logiciel d'être client et serveur en même temps.

Sauvegarde: Opération qui consiste à dupliquer et à mettre en sécurité des fichiers actuels contenus dans un système d'information.

Scam ou arnaque: E-mail/SMS qui essaie d'abuser de la naïveté des internautes qui croient qu'ils ont gagné à une loterie ou un concours afin de leurs escroquer de l'argent.

Signature électronique: Suite de caractères qui permet l'identification d'une personne ou d'une donnée. Elle est utilisée pour vérifier l'intégrité des données et l'identité de l'émetteur.

SMSI *(Système de Management de la Sécurité de l'Information)*: Partie du système de management global, basée sur une approche du risque lié à l'activité, visant à établir, mettre en œuvre, exploiter, surveiller, réexaminer, tenir à jour et améliorer la sécurité de l'information.

ISO/IEC 27001:2005

Sniffer: Programme malveillant installé sur une machine d'un réseau pour écouter le trafic et collecter toutes les informations qui y transitent (exemple: Login, Password).

Spam: E-mail non sollicité par les destinataires, et généralement mensongers (dit aussi « junk mail »), expédié en masse à des fins publicitaires ou malhonnêtes.

Spoofing *(usurpation d'identité électronique)*: Technique qui consiste à usurper l'identité (ou voler l'identité) d'un utilisateur sur Internet (ou au sein d'un réseau en général), afin de faire croire que les actions ou communications

faites proviennent de quelqu'un d'autre (l'utilisateur dont on a usurpé l'identité).

Spyware *(logiciel espion)*: Logiciel parasite indétectable destiné à collecter des informations sur les habitudes de navigation d'un utilisateur ou encore des informations personnelles (adresse e-mail,…), pour des buts « commerciaux malsains » sans avoir une action destructive.

SSH *(Secure Shell)*: À la fois un programme informatique et un protocole de communication sécurisé. Le protocole de connexion impose un échange de clés de chiffrement en début de connexion. Par la suite toutes les trames sont chiffrées. Il devient donc impossible d'utiliser un sniffer pour voir ce que fait l'utilisateur.

Stateful inspection *(filtrage de paquets dynamique)*: Architecture avancée de pare-feu qui a été inventé par Check Point Software Technologies au début des années 1990. Il a remplacé le filtrage de paquets statique.

Certains protocoles dits « à états » comme TCP introduisent une notion de connexion. «Stateful firewall» (les pare-feu à états) vérifient la conformité des paquets à une connexion en cours. C'est-à-dire qu'ils vérifient que chaque paquet d'une connexion est bien la suite du précédent paquet et la réponse à un paquet dans l'autre sens. Ils savent aussi filtrer intelligemment les paquets ICMP qui servent à la signalisation des flux IP.

Switch *(commutateur réseau)*: Equipement qui relie plusieurs segments (câbles ou fibres) dans un réseau informatique. Il s'agit le plus souvent d'un boîtier disposant de plusieurs (entre 4 et 100) ports Ethernet.

TypoSquatting: Forme de cybersquattage se fondant principalement sur les fautes de frappe commises par les internautes au moment de saisir une adresse web dans un navigateur.

Ver *(Worm)*: Type de virus qui se propage à travers un réseau.

Virus: Programme de très petite taille qui possède la faculté de s'introduire dans un programme hôte, et de s'auto-reproduire chaque fois que celui-ci démarre. Son but est généralement de détruire ou de falsifier des fichiers de données ou des fichiers de systèmes d'exploitation.

VPN *(Virtual Private Network ou réseau privé virtuel ou RPV)*: Ensemble de réseaux qui apportent des services de sécurité complémentaires à ceux offerts par les

firewalls. Ils garantissent l'intégrité et la confidentialité des données échangées entre sites distants via Internet ou des réseaux publics non sécurisés.

Vulnérabilité ou faille: Faiblesse d'un bien ou d'un groupe de biens pouvant faire l'objet d'une menace. ISO/IEC 27002:2005

WEP *(Wired Equivalent Privacy)***:** Protocole pour sécuriser les réseaux sans fil de type Wi-Fi. Les réseaux sans fil diffusant les messages échangés par ondes radioélectriques, sont particulièrement sensibles aux écoutes clandestines. Le WEP tient son nom du fait qu'il devait fournir aux réseaux sans fil une confidentialité comparable à celle d'un réseau local filaire classique.

WI-FI ou Wireless Fidelity ou Ethernet sans fil: Technique de réseau informatique sans fil mise en place pour fonctionner en réseau interne et, depuis, devenu un moyen d'accès à haut débit à Internet. Il est basé sur la norme IEEE 802.11. ISO/CEI 8802-11.

WAP *(Wireless Application Protocol)***:** Protocole de communication dont le but est de permettre d'accéder à Internet à l'aide d'un appareil de transmission sans fil, comme par exemple un téléphone portable, un assistant personnel, etc.

XSS *(Cross Site Scripting)***:** Attaque qui exploite les vulnérabilités de pages web dynamiques (écrites en PHP, ASP ou JSP).

IMAGE CONSEIL 71 849 152

ActiveX
Adresse IP
ANSI (Agence Nationale de la Sécurité Informatique)
ANSI (American National Standards Institute)
Anti-virus
Appliance
Archivage électronique
Attaque
Audit sécurité
Authentification
Backdoor (Porte dérobée)
Backup
Biométrie
Black List (liste noire)
Bombe logique
Brute Force
Botnet (réseau Zombie)
Certificat électronique
CERT (Computer Emergency Response Team)
Cheval de Troie (troyen ou trojan horse)
Chiffrement (cryptage)
Code source
Cookie
Confidentialité
Contournement de la politique de sécurité
Contrôle d'accès
Clé
Clonage de serveur DNS (DNS pharming)
Cryptanalyse