LES ATTAQUES INFORMATIQUES ET LEURS PARADES

ATTAQUE	TERME ANGLAIS	DESCRIPTION ET ACTION EVENTUELLE	PREVENTION	CORRECTION	ATTAQUES SIMILAIRES
Bombardement E-mail	E-mail bombing	Attaque visant à saturer une boîte à lettres électronique par la transmission de messages en grand nombre. Cette attaque peut non seulement bloquer la boite au lettre attaquée mais risque de bloquer le serveur complet.	Filtre anti-spam, mise à jour logiciels du serveur.	Selon la gravité de l'attaque, effacer les messages transmis, sinon, réinstaller la boite au lettre d'après les dernières sauvegardes.	Dénis de service, Inondation
Bombe logique	Logic bomb	Partie de code informatique malveillant, insérée au sein d'un logiciel fonctionnel, normalement dormant, mais se déclenchant suite à un évènement ou à une date précise.	Pour les spécialistes: analyse de code, système d'assurance qualité. Utilisateurs: Ne pas installer des logiciels inconnus ou piratés. Avoir un Anti-virus à jour.	Trouver les codes défectueux du source et les retirer. Déconnecter son ordinateur du réseau. Vérifier les autres machines du réseau. Désinstaller tous les logiciels inconnus ou piratés. Balayer tous ses disques avec un logiciel anti-virus à jour.	Cheval de Troie, exploit.
Cassage de mot de passe	Password cracking	Opération consistant à recouvrir le mots de passe d'un utilisateur légitime d'un système, permettant à son auteur de s'introduire dans le système sous l'identité de l'utilisateur.	Utiliser des mots de passe difficile à casser: 8 caractères min, minuscules, capitales, signes. Ne jamais les divulguer à d'autres, ne pas les afficher dans son bureau, et en changer régulièrement.	Changer le mot de passe de l'utilisateur et de tous ceux auxquels l'intrus aurai pu avoir accès.	Intrusion réseau, capture de trafic, usurpation d'identité.
Canular	Hoax	Pas réellement une attaque, un canular est une histoire fausse ou une chaîne qui prend inutilement des ressources informatiques et l'attention des internautes.	Filtre anti-spam	Effacer le message, surtout ne pas le retransmettre.	Spam
Capture de trafic	Sniffing	Ecoute active ou passive avec un logiciel permettant de capturer le trafic d'un Internaute, et éventuellement ses mots de passe.	Utiliser des liaisons cryptées pour toutes les données privées (VPN, https, etc..)	La prévention est la seule mesure efficace. En informer le service informatique afin de refermer la brèche de sécurité.	Divulgation d'informations personnelles.
Cheval de Troie	Trojan Horse	Logiciel malveillant d'apparence légitime conçu pour exécuter des actions à l'insu de l'utilisateur. Il peut par exemple chercher à gagner des droits administrateurs, transmettre des informations privées, ou permettre une intrusions par Internet.	Utilisateurs: Ne pas installer des logiciels inconnus ou piratés. Avoir un Anti-virus à jour.	Déconnecter son ordinateur du réseau. Vérifier les autres machines du réseau. Désinstaller les logiciels inconnus ou piratés, balayer tous ses disques avec un logiciel anti-virus à jour, installer les dernières mises à jour du système d'exploitation. Dans certains cas, il est nécessaire de réinstaller le système d'exploitation et les logiciels à partir des sources d'origine.	Bombe logique, divulgation d'informations personnelles, exploit.
Dénis de service	Denial of Service - DOS	Une attaque par dénis de service d'un serveur a pour but d'arrêter son bon fonctionnement. Ce sont souvent des attaques par saturation, utilisant parfois des failles de sécurités ou exploits. L'utilisation de réseau important de machine Zombie rend l'attaque difficilement parable.	Eviter de devenir une machine Zombie, mise à jour du système d'exploitation, pare feu activé et bien configuré. Technicien: Vérifier les log du pare feu central.	Pour le technicien pendant l'attaque: Identifier la ou les sources et bannir leur adresse IP sur le pare-feu central. Le serveur peut ne pas redémarrer correctement après une telle attaque et nécessiter un redémarrage.	Machine Zombie, inondation, Exploit.
Risque de divulgations d'informations personnelles	Privacy risks	Ensemble d'actions pouvant d'entraîner la diffuser d'informations personnelles. Du navigateur Internet communiquant des informations, au logiciel malveillant transmettant des mots de passe.	Utilisateurs: Utiliser un niveau de sécurité élevé de son navigateur Internet, crypter ses données confidentielles, passer par un proxy d'anonymat pour surfer, toujours utiliser des sites web sécurisés (https) pour rentrer ses données personnelles. Techniciens: effacer définitivement les donnés des disques dur, bande magnétiques, clef USB mises au rebut.	La prévention est la seule mesure efficace. La prévention est la seule mesure efficace.	Hameçonnage, Ingénierie social, Usurpation d'identité, enregistreur de frappe, fuite de données.
Enregistreur de frappe	Keystroke Logging	Logiciel espion enregistrant les touches frappées sur le clavier d'un ordinateur, pouvant soit les garder sur un fichier local, soit les transmettre via Internet.	Ne pas utiliser des ordinateurs à accès public qui auraient pu être piégés, anti-virus à jour, OS à jour, pare feu activé et bien paramétré.	La prévention est la seule mesure efficace.	Hameçonnage, Ingénierie social, Usurpation d'identité.
Exploit	Exploit	Programme malveillant utilisant une faille de sécurité pour permettre à son auteur de prendre le contrôle de l'ordinateur.	Ne pas installer de logiciels inconnus ou piratés, maintenir le système d'exploitation et l'anti virus à jour, pare feu activé et bien paramétré. Utiliser des processeurs récents, équipés de protection efficace contre certaines des attaques d'exploit. Ne pas télécharger de fichiers pouvant être infectés par des virus.	Déconnecter son ordinateur du réseau. Désinstaller les logiciels inconnus ou piratés, balayer tous ses disques avec un logiciel anti-virus à jour, installer les dernières mises à jour du système d'exploitation. Dans certains cas, il est nécessaire de réinstaller le système d'exploitation et les logiciels à partir des sources d'origine.	Machine Zombie, dénis de service, virus.

LES ATTAQUES INFORMATIQUES ET LEURS PARADES

ATTAQUE	TERME ANGLAIS	DESCRIPTION ET ACTION EVENTUELLE	PREVENTION	CORRECTION	ATTAQUES SIMILAIRES
Fuite de donnée	Data spill	Décrit la diffusion non intentionnée d'information sensible. Cela inclus par exemple la vente ou la mise au rebut d'ordinateur dont les données n'ont pas été effacées, les cassettes de sauvegarde jetées sans avoir été effacées, la perte d'ordinateurs ou de supports de données (clef USB), des fichiers envoyés par E-mail alors qu'ils ne devraient pas, des documents mis sur des pages , etc..	Procédures de sécurité renforcées sur les données sensibles, cryptage des données et des liaisons, effacement systématique des supports de données devant être jetés, responsabilisation des utilisateurs, utilisation systématique de clef USB cryptées pour l'extérieur, authentification biométrique sur les PC portables.	La prévention est la seule mesure efficace.	Hameçonnage, Ingénierie social, usurpation d'identité, enregistreur de frappe, risque de divulgations d'informations personnelles.
Hameçonnage, filoutage	Phishing	Technique de fraude cherchant à obtenir des informations confidentielles, telles des mots de passe ou des numéros de carte de crédit, à l'aide de messages électroniques ou de sites usurpant l'identité d'entreprises ou d'institutions financières. Les informations recueillies sont alors utilisées pour récupérer de l'argent ou des informations confidentielles.	Être extrêmement prudent à la réception de message de ces institutions, particulièrement s'ils demandent de se rendre sur leur site pour vérifier votre identité. Passer la souris sur le lien vers le site pour vérifier s'il pointe bien vers la bonne adresse. Une fois sur le site, vérifier son adresse en ouvrant l'onglet fichier / propriété. Mettre à jour son navigateur dont les dernières versions disposent d'un filtre anti hameçonnage. Utiliser un filtre anti spam à jour. En cas de doute, contacter l'institution en question directement avant de répondre au message.	Changer le mot de passe de l'accès à l'institution immédiatement, vérifier les transferts. Porter plainte si des transfert d'argent ou d'information on déjà eu lieu.	Ingénierie social, usurpation d'identité, enregistreur de frappe, risque de divulgation d'information personnelles.
Ingénierie social	Social engineering	Le terme regroupe toutes les techniques de manipulation visant à obtenir des victimes une information ou une action particulière au profit de leur auteur. En utilisant la supercherie, le charisme, l'imposture ou son culot, le hacker abuse de la confiance, de l'ignorance ou de la crédulité de personnes possédant ce qu'il tente d'obtenir.	Être très prudent face à toute demande pouvant résulter d'une brèche de sécurité. Ne jamais communiquer son mot de passe.	La prévention est la seule mesure efficace.	Usurpation d'identité, risque de divulgation d'informations personnelles, hameçonnage.
Inondation	Flooding	Attaque par saturation d'un serveur informatique. L'attaquant utilise souvent des machines Zombies pour multiplier les sources d'attaque et ainsi son efficacité.	Eviter de devenir une machine Zombie, mise à jour du système d'exploitation, pare feu activé et bien configuré. Technicien: Vérifier les log du pare feu central.	Pour le technicien pendant l'attaque: Identifier la ou les sources et bannir leur adresse IP sur le pare-feu central. Le serveur peut ne pas redémarrer correctement après une telle attaque et nécessiter un redémarrage.	Dénis de service, bombardement E-mail.
Intrusion réseau	Intrusion	Ce terme regroupe toutes les techniques permettant à un attaquant de pénétrer dans un système informatique. Cela inclus l'utilisation de brèches de sécurité dans les serveurs, la dépose d'un cheval de Troie, etc..	Analyse de sécurité, utilisation d'un système de détection d'intrusion, mise à jour des systèmes d'exploitation et anti-virus, informations utilisateurs. Ne pas ouvrir de fichier attaché douteux à des E-mail.	La prévention est la seule mesure efficace. Supprimer la cause si une intrusion s'est déroulée.	Hameçonnage, ingénierie social, cheval de Troie.
Logiciel espion, mouchard	Spyware	Logiciel malveillant s'installant dans un ordinateur dans le but de collecter et de transférer des informations à son auteur. Le but en est souvent le profilage dans un but commercial, mais il peut aussi être frauduleux. Les spyware accompagnent certains logiciels gratuits, surtout ceux proposés dans des fenêtres de publicité insistantes lors de la visite de certains sites .	Ne jamais installer un logiciel proposé avec insistance par certaines publicités, n'installer que des logiciels connus, et surtout pas des versions piratées. Utiliser un logiciel anti-virus à jour, faire régulièrement un balayage de son disque dur avec des logiciels anti-malware comme Spybot ou Adware. Ne pas ouvrir de fichier attaché douteux à des E-mail	Balayer son disque dur avec un logiciel anti spyware comme Adware ou Spybot.	Cheval de Troie, exploit, risque de divulgation d'information et d'usurpation d'identité.
Logiciel malveillant	Malware	Logiciels destinés à nuire à un système informatique. On trouve sous ce terme les virus, vers, mouchard, bombe logique et chevaux de Troie.	Ne jamais installer un logiciel proposé avec insistance par certaines publicités, n'installer que des logiciels connus, et surtout pas des versions piratées. Utiliser un logiciel anti-virus à jour, faire régulièrement un balayage de son disque dur avec des logiciels anti-malware comme Spybot ou Adware. Utiliser un pare feu bien configuré. Ne pas ouvrir de fichier attaché douteux à des E-mail. Voir les actions spécifiques aux bombes logiques.	Déconnecter son ordinateur du réseau. En fonction du logiciel, balayer son disque dur avec un logiciel anti-virus ou un anti spyware comme Adware ou Spybot.	Virus, vers, mouchard, bombe logique, chevaux de Troie, machine zombie

LES ATTAQUES INFORMATIQUES ET LEURS PARADES

ATTAQUE	TERME ANGLAIS	DESCRIPTION ET ACTION EVENTUELLE	PREVENTION	CORRECTION	ATTAQUES SIMILAIRES
Machine Zombie	Zombie computer	Ordinateur contrôlé à distance par un pirate informatique à l'insu de son utilisateur. Ces machines sont souvent utilisés pour attaquer d'autres machines, par exemple par déni de service ou pour envoyer des pourriels. Le contrôle de la machine s'effectue via un logiciel malveillant, cheval de Troie, vers ou virus. On appelle Botnet un réseau de machines Zombie.	Ne jamais installer un logiciel proposé avec insistance par certaines publicités, n'installer que des logiciels connus, et surtout pas des versions piratées. Utiliser un pare feu bien configuré. Ne pas ouvrir de fichier douteux attaché à des E-mail. Utiliser un logiciel anti-virus à jour, faire régulièrement un balayage de son disque dur avec des logiciels anti-malware comme Spybot ou Adware.	Déconnecter son ordinateur du réseau. Vérifier les autres machines du réseau. Balayer son disque dur avec un logiciel anti-virus ou un anti spyware comme Adware ou Spybot.	Virus, vers, mouchard, bombe logique, chevaux de Troie, logiciel malveillant, porte dérobée, rootkit, shellcode.
Porte dérobée	Backdoor	Fonctionnalité inconnue de l'utilisateur légitime donnant un accès secret à un logiciel. Cette fonctionnalité peut exister dans le programme d'origine, soit être ajoutée par un virus ou un ver. L'attaquant peut ainsi prendre le contrôle de la machine pour en faire un zombie, accéder à un réseau et récupérer des informations confidentielles.	Ne jamais installer un logiciel proposé avec insistance par certaines publicités, n'installer que des logiciels connus, et surtout pas des versions piratées. Utiliser un pare feu bien configuré. Ne pas ouvrir de fichier douteux attaché à des E-mail. Utiliser un logiciel anti-virus à jour..	Balayer son disque dur avec un logiciel anti-virus.	Virus, vers, mouchard, bombe logique, chevaux de Troie, logiciel malveillant, shellcode, rootkit.
Pourriel, polluriel	Spam	Message électronique non sollicité envoyé en masse, dans un but publicitaire, malhonnête ou agaçant. Ces messages peuvent contenir des logiciels malveillants. Ils peuvent également être utilisé pour l'hameçonnage frauduleux.	Disposer d'un logiciel anti-spam bien configuré sur sa messagerie, un anti-virus bien à jour. Etre très prudent avec les fichiers attachés ou les messages dont l'origine n'est pas clairement identifiée et connue.	Des plaintes peuvent être déposés auprès des entreprises connectant les auteurs de pourriel à l'Internet, mais elles n'ont que peut d'effet jusqu'à présent. Voir les actions contre les virus en cas d'infection.	Virus, vers, mouchard, logiciel malveillant, cheval de Troie, hameçonnage.
Publiciel	Adware	Logiciel fonctionnel qui affiche de la publicité lors de son utilisation. Beaucoup de publiciels sont des logiciels utiles dont la publicité sert à payer le développement, certains contiennent des logiciels espions transmettant les habitudes de l'utilisateur afin de leur envoyer des publicités ciblées.	Ne jamais installer un logiciel proposé avec insistance par certaines publicités, n'installer que des logiciels connus, et surtout pas des versions piratées. Utiliser un logiciel anti-virus à jour, faire régulièrement un balayage de son disque dur avec des logiciels anti-malware comme Spybot ou Adware. Ne pas ouvrir de fichier douteux attaché à des E-mail	Déconnecter son ordinateur du réseau. Vérifier les autres machines du réseau. Désinstaller les logiciels inconnus ou piratés, balayer tous ses disques avec un logiciel anti-virus à jour, installer les dernières mises à jour du système d'exploitation.	Virus, vers, mouchard, logiciel malveillant, cheval de Troie, hameçonnage.
Rootkit	Rootkit	Programme ou ensemble de programme permettant à un tiers de maintenant l'accès à une machine déjà compromise. En agissant au niveau du système d'exploitation, le rootkit camoufle l'intrusion et la porte dérobée, ce qui rend la détection de l'ensemble difficile.	Il faut éviter que sa machine soit compromise, dont ne jamais installer un logiciel proposé avec insistance par certaines publicités, n'installer que des logiciels connus, et surtout pas des versions piratées. Utiliser un logiciel anti-virus à jour, faire régulièrement un balayage de son disque dur avec des logiciels anti-malware comme Spybot ou Adware. Utiliser un pare feu bien configuré. Ne pas ouvrir de fichier attaché douteux à des E-mail. Voir les actions spécifiques aux bombes logiques.	Déconnecter son ordinateur du réseau. Vérifier les autres machines du réseau. Balayer son disque dur avec un logiciel anti-virus spécialisé dans les rootkits comme avast! ou Sophos Anti-Rootkit. La réinstallation du système complet est l'action la plus sure concernant l'éradication du root kit et de la brèche de sécurité.	Virus, vers, mouchard, logiciel malveillant, cheval de Troie, hameçonnage, Shellcode.
Shellcode	Shellcode	Logiciel malveillant permettant de lancer une fenêtre de commande, permettant à l'attaquant de lancer des commandes sur la machine. Un Shell code est souvent la partie active d'un exploit.	Ne pas installer de logiciels inconnus ou piratés, maintenir le système d'exploitation et l'anti virus à jour, pare feu activé et bien paramétré. Utiliser des processeurs récents, équipés de protection efficace contre certaines des attaques d'exploit.	Déconnecter son ordinateur du réseau. Désinstaller les logiciels inconnus ou piratés, balayer tous ses disques avec un logiciel anti-virus à jour, installer les dernières mises à jour du système d'exploitation. Dans certains cas, il est nécessaire de réinstaller le système d'exploitation et les logiciels à partir des sources d'origine.	Virus, vers, mouchard, logiciel malveillant, cheval de Troie, hameçonnage.
Usurpation d'adresse IP	IP spoofing	L'usurpation d'adresse réseau permet à un attaquant de s'introduire sur un réseau dont la seule protection est liée à la détection d'adresse réseau (IP ou MAC).	Ne pas utiliser de service se basant sur l'adresse IP ou MAC pour identifier les clients, mais préférer des systèmes cryptographiques comme SSL.	Ne pas utiliser de service se basant sur l'adresse IP ou MAC pour identifier les clients, mais préférer des systèmes cryptographiques comme SSL.	Intrusion réseau, capture de trafic, usurpation d'identité.

LES ATTAQUES INFORMATIQUES ET LEURS PARADES

ATTAQUE	TERME ANGLAIS	DESCRIPTION ET ACTION EVENTUELLE	PREVENTION	CORRECTION	ATTAQUES SIMILAIRES
Usurpation d'identité utilisateur	Identity Theft	L'attaquant usurpe l'identité d'un utilisateur autorisé dans le but de pénétrer dans un système informatique. L'obtention des renseignements personnels peut s'effectuer par: craquage de mot de passe, écoute, hameçonnage ou autre méthode d'escroquerie (vol, fouille de poubelle, etc..).	Ne jamais utiliser son mot de passe autrement que sur une liaison sécurisée, être très prudent avec ses mots de passe, ne pas mettre au rebus des PC ou des supports de données sans en avoir complètement effacés les données.	Changer le mot de passe de l'utilisateur. Vérifier les autres dégâts éventuels. Vérifier la présence de porte ouverte, root kit ou autre technique permettant à l'attaquant de revenir dans le système. Les supprimer ou réinstaller tous les systèmes à partir des sources d'origine.	Intrusion réseau, capture de trafic, usurpation d'identité, usurpation d'adresse IP.
Vers informatique	Computer Worm	Un vers informatique est un logiciel malveillant qui se diffuse via un réseau informatique. Il peut exploiter les brèches de sécurité laissées ouvertes. Un vers peut espionner l'ordinateur ou il se trouve, mettre en place une porte dérobée, détruire les données ou nuire au fonctionnement au système d'exploitation ou au réseau. Un vers peut être attachée à un message ou intégré à une page Web.	Ne pas installer de logiciels inconnus ou piratés, maintenir le système d'exploitation et l'anti virus à jour, pare feu activé et bien paramétré.	Déconnecter son ordinateur du réseau. Désinstaller les logiciels inconnus ou piratés, balayer tous ses disques avec un logiciel anti-virus à jour, installer les dernières mises à jour du système d'exploitation.	Virus, mouchard, logiciel malveillant, cheval de Troie, hameçonnage, Shellcode.
Virus informatique	Computer virus	Programme malveillant qui une fois activé cherche à infecter d'autres logiciels sur l'ordinateur ou il se trouve. Ils peuvent être diffusés par téléchargement de programme sur Internet, E-mail ou par des supports de données déjà infectés (clef USB, CDROM, etc..).	Ne pas ouvrir de fichier douteux attaché à des messages. Ne pas installer de logiciels inconnus ou piratés, maintenir le système d'exploitation et l'anti virus à jour. Régler le niveau de sécurité macro de word au maximum.	Déconnecter son ordinateur du réseau. Désinstaller les logiciels inconnus ou piratés, balayer tous ses disques avec un logiciel anti-virus à jour, installer les dernières mises à jour du système d'exploitation.	Vers, mouchard, logiciel malveillant, cheval de Troie, hameçonnage, Shellcode.
Date: 22.08.2009					