DEBUTER LE HACKING

</>

BENOIT REPLAY

Grand passionné de livres, je vous partage mes lectures afin que vous puissiez apprendre le principal. Si vous aimez ce que je réalise, n'hésitez pas à me le dire en me laissant un message.

Bonne Lecture

Benoît.

A ma petite famille qui me soutient dans cette fabuleuse aventure…

Le contenu de ce livre vous est distribué à titre informatif. Je décline toutes responsabilités quant à vos actions !

SOMMAIRE

Au cœur de notre société.

C'est au cours des années 1970 que le Hacking voit le jour. Depuis, cette pratique n'a cessé d'évoluer représentant une menace de taille pour la durabilité des entreprises dans un contexte où l'échange des données et l'utilisation des supports numériques se multiplient. En cela, la sécurité des systèmes informatique est un véritable défi pour les spécialistes du genre.

Parmi ses représentants les plus connus, nous retrouvons le groupe Anonymous. Ce dernier revêtant l'habit d'un mouvement activiste qui au nom de certaines valeurs dénonce des atteintes aux libertés individuelles ou collectives. Le Hacking dans ce contexte est motivé par la défense d'idéologies ou philosophies politiques.

Quant aux sociétés informatiques, elles reconnaissent bien volontiers le génie de ces pirates aussi n'hésitent-ils pas à faire appel à leurs services notamment pour assurer la sécurité de leurs logiciels.

Si le hacking déchaine les passions, cette pratique reste cependant illégale et condamnable. Selon une étude de l'entreprise américaine de conseils et de recherches appliquées aux techniques avancées "Gartner", il se peut qu'en 2018, 50% des sociétés mondiales n'aient plus le choix que de faire appel à l'assistance d'un expert en sécurité des systèmes informatiques pour

protéger leurs systèmes.
En effet, les objets connectés et le Cloud sont bien intégrés dans le quotidien des utilisateurs ce qui en facilite l'exploitation des faiblesses par les pirates. Cette réalité n'échappant pas aux écoles dédiées, l'enseignement en Cyber-sécurité occupe une place importante dans leurs programmes même si cela implique forcément de traiter du hacking. Ce qui n'est pas sans déplaire aux entreprises qui y voient là la formation de meilleurs professionnels informatiques.

Certains d’entre eux sont d’ailleurs à l’origine de l’open source et de la philosophie qui le caractérise.
À savoir que l'Open Source est un logiciel, souvent fruit d'une collaboration entre différents programmeurs, dont le code source est proposé en libre accès à la communauté internet. Les membres de cette dernière sont alors invités à y contribuer et ainsi en améliorer la fonctionnalité. Ce logiciel repose sur une idée de partage réciproque et chacun y trouve son avantage. Les bénéfices sont multiples: supports plus réactifs, correction de bugs, ajout de nouvelles fonctionnalités.

Qu'est-ce qu'un hacker ?

Définition

D'après le dictionnaire Larousse, désigne une: "Personne qui, par jeu, goût du défi ou souci de notoriété, cherche à contourner les protections d'un logiciel, à s'introduire frauduleusement dans un système ou un réseau informatique."
Celui-ci faisant acte de détournement, il agit donc illégalement exploitant alors les failles et vulnérabilités d'un système. Il bafoue ainsi de plein fouet et avec une curiosité bien placée l'autorité.
On peut traduire ce terme en français par " bidouilleur", soulignant bien l'activité de détournement dont il fait acte et la liberté dont il fait preuve pour étudier et tester de nouvelles approches.

À savoir que le terme "hacker" qualifie également un grand spécialiste de l’informatique qui emploie ses compétences pour informer les administrateurs des vulnérabilités de leurs systèmes et optimiser leur sécurité.

Les grandes figures du piratage

Nous recensons ci-après quelques pirates célèbres:

- Si nous devons citer un pirate au chapeau noir de renom, c'est bien Kevin Mitnick. Cet américain s'est fait connaitre entre 1980 et 1990 pour s'être introduit dans divers systèmes informatiques. Parmi les entreprises violées, nous pouvons citer: Nokia, Fujitsu, Pacific Bell ou encore Motorola. Son activité est notamment caractérisée par le "phreaking", à savoir le piratage d'infrastructures téléphoniques. Kevin Mitnick a depuis fait acte de repentance et s'est converti en auteur et consultant en sécurité des systèmes informatiques.

- Programmeur américain de jeux, John Carmack est une personnalité reconnue du genre. Il a notamment grandement collaboré au développement de la technologie trois dimensions dans le graphisme des jeux. C'est l'un des fondateurs de la société Id Software, spécialisée dans le développement de jeux vidéo. Les plus grands jeux dont il a été le chef programmeur sont: Doom, Quake ou encore Wolfenstein 3D. Il occupe encore une place d'influence dans le domaine de la technologie.

- En 1991, c'est Linus Torvalds, alors étudiant, qui se distingue en fondant le projet Linux. Ce système d'exploitation qu'il a pu développer via l'Open Source, est l'un des plus utilisés au monde. Libre et complet, ce système peut remplacer Windows ou Microsoft et auquel s'ajoutent des logiciels libres auxiliaires. On retrouve souvent la dénomination Gnu/Linux car Linux est en réalité un noyau qui ne saurait fonctionner sans les logiciels du projet Gnu.

- Dennis Ritchie est une autre figure emblématique du hacking. Père de l'informatique moderne, il est l'inventeur du langage de programmation C et l'un des développeurs du système d'exploitation Unix. À savoir que ce logiciel a permis le développement d'iOS, Apple et Mac OSX. Il nous a quittés en 2011.

Les différents types de pirates

Le hacking revêt différentes catégories qui renvoient à l'image du bon et du mauvais si propre aux westerns.

Les White Hats

Nous distinguons tout d'abord les White Hats ou pirates aux chapeaux blancs: le groupe des gentils. Dénommés également " pirates éthiques", ils arborent le slogan suivant: "apprendre l’attaque pour mieux se défendre". Les White Hats emploient leurs compétences au service de la communauté cela leur valant l'acceptation des membres de la société.
Administrateurs réseaux, consultants en sécurité, lutte contre la cybercriminalité ou adeptes de l'open source, telles sont les activités qui leurs sont généralement attribuées. Qu'il s'agisse d'un autodidacte ou d'un professionnel reconnu, l'approbation des membres de la communauté est essentielle afin de recevoir ce titre de pirate au chapeau blanc. De plus, il faut partager une certaine culture et s'investir dans des projets open source. Ils aident en quelque sort les autres membres à se défendre.

Les Black Hats

Nous retrouvons par la suite les Black Hats ou pirates aux chapeaux noirs: le clan des méchants. Les Black Hats emploient leur intelligence à des fins

malveillantes en détournant les systèmes d'informations. Il s'agit de la communauté des "pirates du web" dont les activités tournent principalement autour du pillage de données, piratage de comptes et introduction frauduleuse dans les systèmes. La menace au virus est une autre de ses caractéristiques qui touche l'ensemble des utilisateurs d'internet.
D'où l'intérêt de bien distinguer la notion de pirate propre aux Blacks Hats et ne pas les confondre avec les pirates éthiques.
Sont visés notamment des organisations telles que la NASA, les réseaux d'entreprises et gouvernementales ou encore les serveurs sensibles d'internet.
À savoir que cette catégorie est sévèrement punie par la loi.

Les Grey Hats

Nous distinguons par la suite les Grey Hats ou les pirates aux chapeaux gris. Ceux-là comme vous vous en douterez se situent entre les deux groupes définis plus hauts.
S'ils ne sont pas nocifs, ils agissent néanmoins de façon illégale aspirant principalement à être reconnus. Ainsi, les failles relevées dans les systèmes violés seront communiquées aux responsables ou administrateurs.

Hacktivistes et script-kiddies

Enfin, nous pouvons citer deux dernières catégorie de pirates. Il s'agit tout d'abord des hacktivistes dont la motivation est principalement politique. A ce titre, ce sont les entreprises qui sont principalement visées. Les groupes Anonymous et Lulsec font partie de cette catégorie.
En second lieu, nous retrouvons les script-kiddies ou les gamins employant des scripts. Il s’agit le plus souvent d'amateurs tâchant de s'infiltrer dans les systèmes en s'appropriant des outils crées par d'autres. Nul besoin de préciser que les autres communautés ne les considèrent guère à cause de leur manque d'éthique.

Les études pour travailler dans la sécurité informatique

Définition et accès

D'après une définition de l'Onisep, le métier d'expert en sureté informatique repose sur l'étude de la fiabilité du système d'information d'une entreprise afin d'en garantir la sécurité.

Seuls les informaticiens confirmés peuvent accéder à ce poste avec un niveau bac+5 au minimum.
S'orienter vers une filière d'ingénieur est une des principales voies suivies après le bac.
C'est en 3ème année d'étude d'ingénieur que l'on débute généralement l'enseignement propre à la sécurité des systèmes informatiques. En effet, les bac+2 ayant l'opportunité de rejoindre les écoles à cette étape du cursus, ils peuvent alors pleinement suivre le programme lié à cette spécialité. Car celle-ci représente un enseignement de taille de par la vulnérabilité permanente du monde informatique.
Ainsi, former et sensibiliser les étudiants sur ce sujet est devenu primordial pour les écoles. On attend ainsi des futurs spécialistes une transparence à toute épreuve et une veille technologique constante. En effet, les réglementations liées à la sécurité des systèmes informatiques évoluent sans cesse. De la même façon, le spécialiste doit pouvoir développer une vision

d'ensemble et démontrer une certaine réactivité afin d'anticiper les menaces liées aux réseaux et agir au plus vite.

Missions

La mission de l'expert en sécurité informatique est d'étudier un système d'information afin d'en déterminer les points faibles et mettre en place les stratégies adéquates afin d'assurer une sécurité optimale. Les pirates aux chapeaux blancs peuvent également être invités à intervenir de par leurs compétences d'intrusion. À savoir que l'expert opère toujours en fonction la culture de l'entreprise dont il fait partie.

Normes de sécurité, connaissances techniques dans le développement système, administration des réseaux, telles sont les compétences nécessaires afin d'accéder à cette fonction. Antivirus, pare-feu, gestion des mots de passe ou art de la cryptologie, nombreux sont les dispositifs leur permettant de protéger des attaques virales ou préserver la confidentialité des systèmes.

Les sanctions sur le piratage

Si le piratage connait une croissance sans limites dont le combat semble vain, des sanctions existent afin d'en freiner les actions.

Sanctions légales

Les sanctions relatives au piratage sont énumérées dans les articles 323-1 à 323-7 du Code Pénal, loi 88-19 du 5 janvier 1988 et peaufinée par la loi 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

En voici des extraits ci-après:

- Article 323-1: " Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30 000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45 000 euros d'amende. Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 75 000 € d'amende".
- Article 323-2: "Le fait d'entraver ou de fausser le fonctionnement d'un

système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende. Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à sept ans d'emprisonnement et à 100 000 € d'amende."

- Article 323-5: "Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :

1: L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26 ;

2: L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;

3: La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;

4: La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;

5: L'exclusion, pour une durée de cinq ans au plus, des marchés publics ;

6: L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;

7: L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35."

Infractions

Par ailleurs, selon "l'Observatoire national de la délinquance et des réponses pénales", les infractions relatives à l'utilisation illégale d'internet se divisent en deux catégories:

- Nous citerons en premier lieu les infractions liées aux fraudes "traditionnelles" qui sont apparues avec les nouvelles technologies de l'information et de la communication. Nous pouvons ainsi nommer les atteintes à la vie privée, les escroqueries en tous genres, les menaces ou encore la propagande terroriste.
- Viennent ensuite les infractions liées aux systèmes d’information et de traitement automatisé des données, facilitée par l'essor des réseaux informatiques et d’internet. Il s'agit notamment du vol de données ou d'actes d'intrusion sur les sites internet.

Le cas du téléchargement illégal

De nos jours, le téléchargement illégal est devenu chose courante. Il n'en reste pas moins un délit puni par la loi.
Il s'agit de l'utilisation frauduleuse d'une œuvre protégée par des droits d'auteur. Les risques sont d’ordres pénaux. Ce délit de contrefaçon expose l'auteur à une peine pouvant aller jusqu'à 3 ans d'emprisonnement et impliquer 300 000 euros d'amende.

Si les amateurs du genre ont conscience des risques auxquels ils s'exposent, le fait que cette sanction ne soit que guère appliquée les encourage à poursuivre leurs méfaits.

La principale arme utilisée afin de lutter contre cette action illégale est la Haute autorité Hadopi.
Sont concernés les personnes passant par des plates-formes de partage de fichiers pour télécharger.
L'utilisateur repéré reçoit alors un premier e-mail d'avertissement par l'Hadopi à l'adresse correspondant à l'abonnement internet de l'utilisateur.
Cela répond à un souhait de graduation des mesures.

L'utilisateur fautif à la possibilité de réclamer la liste des fichiers litigieux et exposer ses observations via le formulaire de réponse Hadopi mis à sa disposition et qu'il peut télécharger en ligne.

Si récidive au bout de 6 mois, un email est renouvelé à l'attention de l'abonné et est suivi cette fois-ci d'une lettre recommandée.

Si dans un délai d'un an, l'utilisateur réitère son méfait, il est alors informé des risques de poursuites pénales auquel il s'expose via une nouvelle lettre remise contre signature. La commission de protection des droits jugera s'il faut saisir le parquet entrainant alors des poursuites judiciaires pour négligence caractérisée.
L'amende prononcée sera de 1500 euros correspondant aux contraventions de 5ème classe.

À savoir que la suspension de la connexion internet n'est plus appliquée depuis la mise en place du décret du 8 juillet 2013.

Comment se protéger contre les pirates

Si l'intervention d'un professionnel s'avère parfois indispensable, il existe néanmoins des moyens à votre portée afin de prévenir les cyber-attaques et vous protéger du piratage. Ne craignez donc plus d'utiliser votre ordinateur et naviguez en toute sécurité.

Les Anti-Hacks

Un des outils vous permettant de protéger et vérifier la sécurité de votre ordinateur est l'anti-Hacks. Cet outil vous permet d'identifier les faiblesses inhérentes à votre machine notamment les défauts des logiciels que vous manipulez. Parmi les logiciels sujets à vérification, nous pouvons citer: Internet Explorer, Java, Acrobat Reader ou encore Firefox. Il s'agit également de s'assurer que vous détenez bien les logiciels dédiés à la sécurité informatique tels que le pare-feu et l'antivirus.
Ainsi, sont visées par les pirates les données personnelles des utilisateurs afin d'exploiter leurs systèmes.
Cet outil est très apprécié de par sa facilité d'utilisation.

Les anti-virus

Il faut également vous assurer que vous disposez bien du bon anti-virus. Celui-ci vous permettra d'identifier toute démarche d'infiltration par des

pirates. En effet, ces derniers accèdent à votre système via votre adresse IP, obtenant les informations traquées mais ouvrant alors une brèche aux virus et autres programmes frauduleux. À savoir que les antivirus les plus performants restent ceux qui sont payants.

Les pare-feu

Quant au pare-feu, il fait office de filtre contre le trafic entrant et sortant. Là encore, le pirate profite d'une faille dans le pare-feu.

Les mises à jour

Antivirus ou Pare-Feu, il est aussi essentiel de réaliser les mises à jour correspondantes afin d'optimiser la sécurité de votre système d'exploitation. En effet, les dernières versions auront corrigé les failles de l'ancienne version.

Protéger la wifi

Un autre conseil à suivre est de veiller à ce que votre connexion wifi soit éteinte la nuit. Cela freinera les tentatives d'irruption dans votre système car c'est le réseau internet qui fait office de pont.
Attention à bien sécuriser votre wifi en modifiant la clé de votre réseau de WEP à WPA. Le décryptage du premier étant plus aisé pour les pirates.

Le choix du navigateur

Il est judicieux de la même façon d'utiliser des navigateurs sécurisés et dont les mises à jour sont fréquentes. Les plus renommés restent Firefox et Chrome. Celui étant le plus sujet à infections est Internet Explorer. Cet avertissement concerne également les sites internet. Veillez à ce qu'ils soient sécurisés notamment à l'heure de procéder à un paiement.

Le choix du mot de passe

De la même façon, il vous incombe de choisir au mieux votre mot de passe. Les pirates ont plusieurs moyens afin d'accéder à vos informations personnelles. Des logiciels malveillants permettent notamment de décoder vos différents mots de passe. On peut citer le logiciel dont la particularité est le décodage via le dictionnaire. Ce dernier permet de tester tous les mots du dictionnaire à vitesse grand V jusqu'à éventuellement trouver le bon code. À savoir qu'une fois vos données personnelles en mains, les pirates ont la possibilité de revendre les informations obtenues, accéder à vos comptes bancaires ou encore s'approprier votre identité. Ils peuvent également faire acte de criminalité en votre nom.
D'où l'intérêt de choisir un mot de passe compliqué en prenant soin d'y inclure des lettres (minuscules et majuscules), des chiffres mais également des symboles. Un changement régulier de code est également prodigué. Surtout que l'on a tendance à emprunter le même mot de passe sur d'autres plateformes et applications. Inutile de préciser de veiller à effacer les messages de votre boîte mail indiquant votre code et pouvant faciliter la

tâche des pirates.

Faire attention aux e-mails

N'oublions pas ces fameux courriels électroniques dont la pièce-jointe peut cacher un virus. Dès lors que le fichier joint est ouvert, s'exécute un programme malveillant. D'où l'intérêt d'être vigilant et ne pas ouvrir les courriels dont la provenance vous est inconnu et qui éveille vos soupçons. Votre meilleur indice reste la formulation de l'extension, celle-ci présentera l'un des codes suivants si le fichier est corrompu: jpg.exe, pdf.bat ou encore exe.bat.com.

Cacher sa webcam

Il peut enfin être prudent de placer un bout de papier devant votre webcam. Cela freinera tout acte de voyeurisme. Personne ne souhaite voir son image défiler sur le net au détriment de sa volonté.

Les différents types d'attaques des hackers

Avant de conduire son attaque, le pirate réunit un maximum d'informations sur sa proie. Et, tous les moyens sont bons que ce soit légalement ou illégalement.

La voie légale

Si l'on suit la voie licite, on empruntera des plateformes telles que les forums, Google ou un éventuel site/blog de la personne traquée. Internet regorge également de nombreux services légaux accessibles aux pirates. Il s'agit notamment des caches relatifs aux serveurs DNS qui, une fois en possession de l'adresse IP de la victime, permettent d'accéder aux sites consultés par ce dernier.
On peut citer également l'outil WHOIS qui fait en quelque sorte office d'annuaire internet. On peut y consulter des registres permettant d'acquérir des informations sur le propriétaire, un nom de domaine ou une adresse IP. On retrouve de la même façon le registre ARIN (American Registry for

Internet Numbers) qui gère les adresses IP pour l'Amérique du nord, l'Amérique du sud et les Caraïbes.

La voie illégale

La méthode illicite consiste à dérober des informations importantes, à inspecter les poubelles de la victime ou passer par l'ingénierie sociale. Cette dernière méthode se sert de la naïveté du genre humain pour arriver à ses fins. Pour illustration, le pirate trompe sa victime en usurpant l'identité d'une personne connue de ce dernier afin d'obtenir les informations visées. C'est là que peut intervenir le phishing ou hameçonnage qui consiste en une opération d'escroquerie, à l'image du spam, visant à obtenir des données personnelles telles que les identifiants, mots de passe ou les numéros de cartes bancaires. Quant au Spyware ou logiciel espion, il s'agit d'un programme réunissant des données sur le propriétaire de l'ordinateur sur lequel il a été exécuté.
Les informations recueillies à l'insu de la victime sont alors divulguées à la société éditrice du spyware qui en tire un profit financier et lui permet notamment d'établir le profil des utilisateurs à des fins publicitaires. Parmi les nombreuses informations visées: les mots-clés saisis dans les moteurs de recherche, les données de cartes bancaires, l'analyse des achats internet ou encore la quête des URL des sites internet consultés.

Les types d'attaques de pirates

Nous en venons aux différents types d'attaques conduites par les pirates. On en distingue trois: l'attaque directe, l'attaque indirecte par rebond et l'attaque indirecte par réponses.

- On retrouve tout d'abord l'attaque directe. Le pirate attaque directement sa proie via son ordinateur. Les "scriptkiddies" en sont de fervents amateurs. Les programmes empruntés n'apparaissant que légèrement paramétrables, il est plus aisé d'en identifier l'auteur.

- L'attaque indirecte par rebond est très appréciée des pirates de l'informatique. Elle permet de masquer l'adresse IP du malfaiteur et d'utiliser un ou plusieurs ordinateurs intermédiaires alors plus puissants pour réaliser son attaque. C'est le principe du rebond. La source est plus difficile à identifier, c'est souvent l'ordinateur intermédiaire qui est confondu.

- L'attaque indirecte par réponse s'assimile à la technique par rebond à cela près que le pirate transmet une requête à l'ordinateur intermédiaire. La victime exécutera la requête via l'ordinateur intermédiaire et la réponse sera transmise au pirate. Encore une fois, la source s'avère difficilement identifiable.

Les autres types d'attaques

- Attaques conventionnelles:

Les attaques de type conventionnel empruntent comme support principal: Internet et se servent de la crédulité des victimes afin d'obtenir des informations personnelles et les exploiter illégalement. Il s'agit des fraudes à la carte de crédit, des menaces et escroqueries en tous genres, de l'usurpation d'identité, de l'extorsion de fonds ou encore du détournement de mineurs.

Cupidité financière et matérielle, immoralité ou malsaine (à travers le racisme ou la pédophilie), telles sont les motivations amenant à commettre ces délits dits " traditionnels".

- Attaques technologiques:

Ce genre d'attaque tire profit des faiblesses et des failles d'un système. Des programmes espions peuvent être installés, des sites internet détériorés, des services internet rendus indisponibles (ou déni de services), des actes d'intrusions ou des vols d'informations exécutés.

Ces attaques sont motivées cette fois-ci par des aspirations stratégiques (vol d'informations confidentielles), cupides (avidité financière ou matérielle), terroristes (contre l'ordre instauré) ou encore idéologiques. La vengeance pour X raison est également une source de motivation.

- Attaques opportunistes:

Ce type d'attaque a pour vocation la multiplication du nombre de victimes. Personne n'est visé en particulier.
On retrouve la création ou l'acquisition d'un logiciel malveillant offrant au pirate un contrôle total sur l'ordinateur de sa ou ses victimes.

- Les Spams

On peut citer également l'envoi ou la location d'un service de spam. Si l'on souhaite atteindre un large public, il faut savoir emprunter le bon canal. Ainsi, une méthode appréciée des pirates est l'envoi de courriels électroniques ou de spams (courriels indésirables).

- Création de sites malveillants

Les pirates peuvent également avoir la mauvaise idée de créer des sites malveillants ou d'infecter des sites existants. Ils affichent alors une présence malsaine sur le net. Cela passe par la mise en place de sites d'arnaques, de phishing, de création de publicités dont l'exploit vise à contaminer les systèmes des internautes.

- Les attaques ciblées

Les attaques des malfaiteurs peuvent être ciblées. En concentrant son action sur une victime, le pirate accentue ses chances d'arriver à ses fins. Toute une procédure est généralement suivie.
Il s'agit tout d'abord de récolter des informations sur le profil de la victime. Dans le cas d'une personne morale, sont visés notamment des courriels ou

des listes de numéros de téléphone affichés sur le net. Les pirates peuvent par la suite procéder à un balayage du réseau. Celui-ci consiste à s'assurer que le système est bien actif et en identifier les failles. À savoir que cette technique peut vite être détectée générant une alerte.
Le fichier piégé est une autre approche prisée des pirates. L'un des plus connus étant le "Cheval de Troie".

- Le Cheval de Troie

Il s'agit d'un logiciel invisible comportant une fonctionnalité malveillante qui via l'exécution d'un fichier viole la sécurité de votre ordinateur et en ouvre l'accès aux pirates. On dit généralement que ces derniers pénètrent dans le système par la " porte dérobée".
Le programme parait sain au premier abord c'est pourquoi il représente une réelle menace pour les utilisateurs d'internet.
Parmi les dégâts dont il est capable, nous retrouvons la copie de données personnelles ou encore le vol de mot de passe.
À savoir que le pirate doit être en possession de votre adresse IP afin de pouvoir s'infiltrer sur votre ordinateur.
Des symptômes vous permettent de reconnaitre la présence de ce logiciel malicieux:
- Plantages quotidiens
- La souris qui fait des siennes
- Chargement de données non choisi
- Des programmes qui s'ouvrent à l'improviste.

Un des meilleurs outils afin de se prémunir contre le cheval de Troie est le pare-feu. Il s'avère alors essentiel de refuser l'exécution d'un programme clamant l'ouverture d'une connexion si celui-ci vous parait inconnu.
Enfin, il existe des programmes vous permettant de les détecter et ainsi les évincer tels que Trojan remover ou The cleaner.

- L'APT

La "menace persistante avancée" que l'on connait sous le sigle APT (Advanced Persistent Threat), est une attaque illustrée par le fait qu'une personne accède frauduleusement à un réseau sans être détecté pendant une longue durée. Cela lui permet de dérober des informations sans forcément s'attaquer au réseau. La défense nationale ou la finance, tels sont les secteurs prisés par les pirates empruntant cette méthode. En effet, les informations y ont une importante valeur.

- Le Sniffing

Le "reniflement de trafics" communément appelé Sniffing est une technique d'espionnage utilisée par les pirates sur le réseau. Il s'agit de récupérer frauduleusement des mots de passe et autres données confidentielle en localisant les messages ou paquets circulant sur le réseau. L'identité des utilisateurs est de la même façon affichée. La faible sécurité d'un protocole facilite le travail du renifleur. On peut citer pour exemple: la DNS (Domain Name System), le FTP (File Transfert Protocol),) ou encore le HTTP (Protocole de transfert hypertexte).

- La force brute

Cette méthode de décodage de mots de passe repose sur le parcours de toutes les combinaisons possibles une à une et de façon exhaustive.
Sont ainsi calculées les empreintes de toutes les combinaisons de caractères existantes et qui seront comparées à l'empreinte visée. Le mot de passe est trouvé dès lors que les deux mots de passe sont identiques.
Le seul inconvénient est que cette méthode peut prendre du temps.

- Rainbow table

À mi-chemin entre la force brute et l'attaque au dictionnaire, la table arc-en-ciel consiste à récupérer un mot de passe à partir de son empreinte. L'idée est tester toutes les combinaisons possibles. Le temps de calcul s'en retrouve fortement réduit. Néanmoins, la capacité du processeur peut imposer des limites, moins le mot de passe a de caractères, plus il sera aisé de le décoder. Au-delà de 14 caractères cela prend beaucoup plus de temps.

Les logiciels et systèmes utilisés

Afin de mener à bien son action de hacking, il est indispensable pour le pirate de choisir les bons logiciels et le bon système d'exploitation. En voici une petite liste:

Kali Linux

Parmi les nombreuses distributions de Linux, nous pouvons citer le logiciel Kali Linux qui fait partie des plus utilisés. Cet OS offre ce qu'il y a de mieux en matière de confidentialité et de sécurité contre les fragilités d'un système. Il s'agit d'une plateforme d'audits de sécurité et de tests d'intrusion. Elle répond aux standards de de développement Debian. Ce dernier représentant un système d'exploitation libre regroupant plus de 51000 paquets ainsi qu'un gestionnaire de paquets et dont la fiabilité n'est plus à prouver.

BlackTrack

BackTrack, qui a précédé Kali Linux, est toujours d'actualité et constitue l'un des systèmes les plus performants en matière de piratage réseau et pentesting (tests d'intrusion).

John The Ripper

Logiciel Open Source, John The Ripper, est spécialisé dans la casse de mots de passe. Ce logiciel permet de vérifier toutes les combinaisons grâce à une liste de mots ou via un mode incrémental jusqu'à trouver la bonne correspondance. C'est un moyen de vérifier la sécurité des mots de passe.

Cain & Abel

Parmi les logiciels gratuits, nous retrouvons Cain & Abel fonctionnant sous Windows et dont l'objet est de récupérer les mots de passe. Les méthodes principalement empruntées sont le cassage de mots de passe ou le sniffing. Sont appréciées les attaques " tables arc-en-ciel" (rainbow tables) et par dictionnaire.
Pour les experts en sécurité, l'idée est de tester la capacité d'un réseau à se défendre contre ce genre d'attaque.

Pentoo

Autre distribution de Linux et basé sur l'Open Source, le logiciel Pentoo prend la forme d'un livre CD spécialisé dans les tests d'infiltration. Nul besoin d'installation, il ne vous reste qu'à lancer son application sur votre ordinateur.

BackBox

Il s'agit à nouveau d'une distribution Linux, basée sur le système d'exploitation Ubuntu, qui réunit différents outils d'analyse et permet de concevoir un environnement préservant la vie privée. Ce système est apprécié pour sa rapidité et sa facilité d'utilisation. Les experts en sécurité s'en servent pour faire des tests de fiabilité et de violation de systèmes.

Nessus

Disponible sous Windows, Mac et Linux, Nessus est un logiciel gratuit qui permet de scanner et de tester la vulnérabilité d'une machine puis d'en corriger éventuellement les failles. S'y ajoutent des plugins aspirant à analyser les antivirus ou les pare-feu.

Nmap

Autre logiciel basé sur l'Open Source, Nmap a pour objet de scanner et ainsi déceler les ports ouverts d'un système. Il s'agit également de rassembler des données sur le système d'exploitation d'un pc distant. Les experts de la sécurité à travers ce logiciel vont détecter les faiblesses du système pouvant attirer les convoitises des pirates du web.

Wireshark

Héritier d'Ethereal et basé sur l'Open Source, Wireshark se présente sous la forme d'un analyseur de protocoles réseau ou " sniffer". Il a pour objet de scanner l'activité d'un réseau et de capter les paquets qui y transitent afin de les analyser. Il permet de repérer les protocoles tels que: HTTP, NETBIOS, FTP ou encore ICQ. Il est apprécié des experts de sécurité à l'heure de réaliser des tests d'intrusion.

Metasploit

Il s'agit d'un outil Open Source dont l'action est de développer des exploits à l'encontre d'une machine distante et d'identifier les failles d'un système afin de s'y introduire et l'exploiter.
Il permet de développer ses propres exploits. Les experts en sécurité l'utilisent afin d'opérer des audits en sécurité.

Aircrack-ng

Il s'agit d'un ensemble d'outils de monitoring visant les réseaux sans fil dont l'objet est la capture de paquets IP et le "cassage" de clés WEP et WPA des réseaux WIFI. On l'utilise également en tant que test d'intrusion. Il est développé sous licence GNU GPL.

Burp Suite

Cet outil existe en version gratuite et en version payante. Il permet d'analyser et exploiter des applications web. Il de configure à la manière d'un proxy. Les requêtes HTTP capturées sont analysées puis réécrites par Burp Suite pour être par la suite de nouveau acheminées. Il s'agit encore une fois d'en vérifier le niveau de sécurité.

Zed Attack Proxy

Distribué sous licence GPL et développé en Java, l'outil Zed Attack Proxy (anciennement dénommé WebScarab) a pour objet le contrôle du fonctionnement d'une application en ligne à l'image de Burp Suite et de ré-exécuter des requêtes vers les serveurs Web. Il permet d'identifier de manière automatique certaines vulnérabilités.

Lexique relatif au hacking

Abandonware

L'Abandonware ou "logiciel abandonné" consiste pour un éditeur de jeux vidéo à proposer un ou plusieurs de ses plus vieux jeux en libre téléchargement. À savoir que le ou les jeux en question ne sont plus commercialisés et le service après-vente n'est plus assuré.

Appz

Appz est l'abréviation du terme "applications" avec une faute d'orthographe délibérée sur le pluriel. Il s'agit d'applications commerciales piratées que l'on peut télécharger librement.
On dénombre d'autres termes propres au hacking et utilisant le "z" en tant que pluriel. On peut citer le terme Warez relatif au piratage de logiciels, le terme Gamez lié au piratage de jeux vidéo ou encore le terme Crackz désignant des programmes permettant de casser les codes de systèmes de protections anti-copie des applications commerciales.

BBS (Bulletin Board System)

Le BBS ou "bulletin d'informations" est un serveur de messagerie permettant aux internautes d'y échanger des informations à l'image d'un

forum communautaire. Cela permet notamment de construire une base de données d'informations.
Il représentait autrefois un pc connecté au réseau téléphonique réceptionnant des appels et les emmagasinant sous forme de messagerie.

Bande passante

Ce terme désigne un transfert de données sur une liaison de transmission durant un laps de temps. C'est la mesure de la rapidité que va prendre une quantité d'informations informatiques pour être transmise sur internet.

Beta

La version Beta renvoie à une version primaire ou d'essai d'un logiciel avant de lancer sa distribution. Cela permet d'en souligner les éventuels bugs et de les corriger avant de commercialiser la version finale. On y recense également des commentaires et des suggestions sur les caractéristiques du logiciel.

Big Brother

Le terme Big Brother est employé pour dénoncer l'état de surveillance en place sur le web ainsi que les actions nuisant aux libertés fondamentales et à la vie privée des individus. Cette notion renvoi au célèbre roman de George Orwell: "1984". Cette œuvre évoque un monde totalitaire où les habitants sont manipulés mentalement et contrôlés physiquement par Big Brother. Ce dernier exerce un regard quasi constant et dominant sur la vie privée des habitants.

Bit Coin (unité d'information binaire/pièce de monnaie)

Il s'agit d'une monnaie virtuelle fruit du travail de Satoshi Nakamoto et empruntant le système de paiement " peer-to-peer". C'est à dire que le système d'échange est direct et décentralisé entre les utilisateurs.
De plus, il est régi sans aucune autorité centrale et repose sur l'approbation des nœuds du réseau (programmes relayant les transactions).
La validité de chaque transaction est garantie par leur enregistrement au sein d'un registre public et inaltérable dénommé "blockchain". De la même manière, l'authenticité des transactions est sécurisée par des signatures numériques relatives aux adresses d'envoi autorisant un contrôle absolu concernant l'échange des bit coins.
Il va sans dire que le Bit coin est la monnaie électronique décentralisée la plus utilisée sur le web.

Black Hat Briefing (conférences Black Hat)

Ce terme désigne les rassemblements de pirates ayant lieu dans différentes villes de la planète et permettant d'échanger des opinions et idées nouvelles concernant la sécurité de l'information.

Bug

Désigne une anomalie de fonctionnement touchant un ordinateur ou un

programme informatique.
Le logiciel ne répond plus alors et n'exécute pas ce qui a été demandé. On parle de plantage ou de blocage informatique. Cela peut provenir d'un défaut de programmation.

Busted

Terme employé lorsqu'un pirate est repéré puis arrêté par la police. On dit qu'il a été busted.

Cache

Un cache désigne une zone mémoire d'un ordinateur où sont stockées les pages web consultées récemment sur internet. Il permet de réduire le temps d'affichage des pages web lorsqu'on revient sur des sites déjà visités. Plus besoin d'attendre que la page se recharge.
Néanmoins, il s'avère essentiel de vider le cache d'un ordinateur régulièrement. Cela permet de pouvoir consulter une page web actualisée, d'effacer les traces d'une navigation, d'éviter la saturation de son disque dur ou encore d'améliorer le fonctionnement de certaines applications.

Carding

Désigne le piratage des cartes bancaires. Cette technique a pour objet d'intercepter un numéro de carte bleue comportant une date d'expiration valide. Les paramètres de la puce sont ainsi exploités et modifiées. Le pirate peut ainsi créer des cartes virtuelles et agir frauduleusement.
Des logiciels permettent de procéder au calcul de l'algorithme autorisant cette fraude.

CNIL

Ce sigle désigne la "Commission Nationale de l'Informatique et des Libertés".
Cette autorité administrative indépendante a pour objet de réglementer la constitution des fichiers informatiques et de veiller au respect des lois relatives à l'informatique, aux fichiers et aux libertés. Elle s'assure que les droits de l'homme, les libertés individuelles ainsi que la vie privée soient préservés.
À savoir que la récolte ou le traitement de fichiers de données réalisés dans un but marketing doivent faire l'objet d'une déclaration auprès de la CNIL.

Coder

Un coder est chargé de tout ce qui est relatif au codage (le fait de coder des données) et à la programmation (rédaction de programmes informatiques). Il peut réaliser du cassage de protection ou encore concevoir des logiciels.

Cookie

Ce terme désigne des fichiers de données au format texte installés sur le disque dur de l'internaute par l'action du serveur du site web visité.
Il réunit des données sur la navigation réalisée sur les pages de ce site. Ces informations auront été récoltées soit par la simple consultation du site soit via le renseignement puis la soumission d'un formulaire ou encore lorsqu'on s'identifie avec un login et un mot de passe. Cela facilite l'utilisation ultérieure du site par le même utilisateur, ses préférences ayant été récupérées par le cookie lors de sa visite initiale. Le navigateur peut également avoir mémorisé le mot de passe. De la même façon, lorsqu'on visite de nouveau le même site, les pages peuvent être soumises selon ce qui a déjà été consulté.
Enfin, le cookie est un outil apprécié du marketing car permettant de cibler le comportement et les habitudes des internautes. Ces données peuvent également être utilisées de façon malhonnête notamment dans le cadre de la publicité.
À savoir que les sites web demandent dorénavant l'autorisation préalable de l'internaute au moment pour ce dernier d'accepter des cookies.

Cracker

Il s'agit d'un pirate informatique dont la spécialité est le contournement des protections anti-copies de logiciels sous licence.

Crasher (plantage informatique)

Désigne un Black Hat pirate employant un logiciel dans le but malsain de s'introduire dans un système et faire planter une connexion ou un ordinateur. La crasher agit pour le plaisir effaçant ou altérant les données d'un utilisateur non ciblé.

Cross-site scripting (XSS)

Le "script intersite" désigne une attaque par injection de script malveillant dans une page web vulnérable avec pour objectif de soustraire des informations confidentielles. En pratique, le script se charge et s'exécute sur l'ordinateur dès lors que l'utilisateur visite la page piégée ou clique sur un lien piégé.
Cette attaque aura profité d'une lacune de sécurité d'un site web.

Cryptage (ou chiffrement)

Processus consistant à convertir les données d'une information claire et lisible en chaînes indéchiffrables garantissant la confidentialité des données d'un utilisateur et au moyen d'une clé de chiffrement. Ce dispositif est particulièrement apprécié à l'heure de réaliser un paiement en ligne.

On distingue deux types de cryptage. Tout d'abord, le chiffrement symétrique qui consiste à emprunter la même clé pour à la fois chiffrer et déchiffrer. Quant au chiffrement asymétrique, il implique deux clés différentes: une clé publique destinée au chiffrement et une clé privée pour déchiffrer. L'alliance de cette paire améliore la confidentialité du message car la clé publique ne pourra être déchiffrée qu'avec la clé privée concordante.

Deepweb (web caché)

Désigne l'ensemble du réseau accessible en ligne mais qui n'est pas référencé par les moteurs de recherche classiques.
Il préserve notamment l'anonymat des visiteurs à qui l'accès aura été autorisé.

DDoS attack (Distributed denial of service attack)

Cette "attaque par déni de service" consiste à surcharger la bande passante d'un serveur le rendant ainsi inaccessible. Les requêtes de connexion se retrouvant multipliées cela a pour effet de ralentir le chargement du serveur ou du site internet ou encore d'en épuiser les ressources systèmes.
Ces attaques peuvent être motivées par des intérêts personnels, financiers, économiques ou encore politiques. Il s'agit d'une menace non négligeable.

DNS (Domain Name System)

Un serveur DNS ou système de nom de domaine désigne un annuaire pour ordinateur. L'ordinateur consulte alors le serveur DNS afin de pouvoir accéder à un pc sur le réseau. Il permet d'associer une adresse de nom de domaine que l'on souhaite contacter à une adresse IP.
Le dépôt d'un nom de domaine auprès d’un bureau d'enregistrement et de l'ICANN (voir lexique) est essentiel afin d'apparaitre sur le web d'une autre manière que par une succession de chiffres (adresse IP). Le DNS permet ainsi de mieux caractériser un site web. Il est composé de deux éléments: la

partie précédent le " point" et celle la suivant qui correspond au domaine de premier niveau (il s'agit de "com.", "org" ou encore "net").
À savoir que les serveurs DNS ne sont pas exempts du joug des pirates. En effet, des virus en place sont capables de modifier les paramètres réseaux renvoyant les requêtes DNS vers des serveurs hackés.

Émulateur

Désigne un logiciel dont l'objet est la simulation du fonctionnement d'une machine sur un appareil autre que celui originalement dédié. Le langage initial de la machine est alors traduit dans le langage de la nouvelle machine. Ce logiciel est particulièrement utilisé dans le monde des jeux vidéo, et permet de renouer avec des jeux anciens qui ne fonctionnent originalement que sur des machines ou des consoles qui ne sont plus commercialisés sur le marché.

Exploit

Un exploit est une technique informatique qui consiste à exploiter une brèche de sécurité et ainsi permettre de pénétrer des systèmes. Et cela au moyen d'un programme malveillant. L'exploit peut notamment être mis en action lors de la visite d'un site présentant un code malveillant ou lorsqu'on accède à un fichier corrompu par un code malveillant. Un bon antivirus s'avère essentiel afin de s'en prémunir.

Flaming (propos inflammatoire)

Cette technique consiste à poster des messages intentionnellement offusquant sur un groupe de discussion, réseau ou forum avec la volonté de générer un conflit. "Flames" est le terme emprunté pour désigner ce type de message. Une "flame war" (guerre de messages hostiles) peut éclater lors d'une séquence d'échange de " flames".
Les instigateurs cherchent ainsi à imposer leurs idées par le biais de la provocation ou de la persuasion provoquant alors des réactions sociales.

Google Dorks

Il s'agit d'une méthode permettant d'utiliser un moteur de recherche (Google ou autre) pour identifier des fuites de données confidentielles qui ne sont pas censées être disponible à travers une recherche lambda et qui se

trouvent indexées sur le moteur de recherche. On parle de requête Google Dork. La page ou le mot-clé repéré peut alors renvoyer à une page vulnérable d'un site web.

GPRS (Global Packet Radio Service)

Il s'agit d'un nouveau service de communication sans fil basé sur la norme GSM et permettant de transférer des données par paquets.

Hacktiviste

Ce terme, fusion du terme désignant l'acteur du hacking et du terme activiste, désigne un pirate informatique guidé par des aspirations politiques. Parmi ses actions, nous retrouvons la censure ou la protection de la vie privée.
Ils représentent un vecteur de communication phare en mettant notamment en lumière les actes inhumains ayant lieu dans le monde ou les contradictions relevées dans les systèmes informatiques.
Ils transmettent leurs opinions via le piratage de sites informatiques, en détournant les serveurs, en déformant et en endommageant les données du site visé. Leur action est de ce fait illégale.

Hijacking (ou Vol de session TCP)

Cette technique de piratage consiste à détourner les réglages relatifs au navigateur d'un internaute et ainsi passer pour un utilisateur authentifié. C'est lors de l'identification de l'internaute que les pirates passent à l'action. Peuvent ainsi être modifiées: la page de démarrage du navigateur web ou encore la page de recherche, entrainant la redirection de l'internaute vers des pages non choisies. L'utilisateur peut également être amené à consulter des annonces publicitaires à son insu et à des fins marketings ou augmenter le nombre de visites d'un site.
Les conséquences peuvent en être la saturation des serveurs web par des annonces intempestives.
Une solution pour combattre cette attaque serait de supprimer les entrées non réclamées sur le navigateur.

Hoax (ou canular)

Désigne une information erronée circulant sur le net que ce soit à travers les courriers électroniques ou les réseaux sociaux et aspirant à se propager largement.
L'idée dans les réseaux sociaux est de susciter la révolte, l'approbation ou

encore l'inquiétude.
Lorsqu'il prend la forme d'un e-mail, il a pour objet d'alerter les internautes qu'un virus menace ou de diffuser un autre type d’une information. Il s'agit évidemment de fausses informations mais dont la rédaction et le professionnalisme peut tromper aisément l'utilisateur.

HTML (Hyper Text Markup Langage)

L'HTML ou "Langage de balises hyper texte" désigne un langage informatique employé sur internet et permettant la conception de pages web. Les balises de formatage sont là pour décrire la manière dont un document va être affiché sur le navigateur et les liens qui vont se constituer avec d'autres documents.

ICANN (Internet Corporation for Assigned Names and Numbers)

Organisme dont la responsabilité est de coordonner les identifiants correspondant aux adresses IP et aux noms de domaine au niveau mondial. C'est elle qui attribue les terminaisons liées aux noms de domaine "de premier niveau".

Iframe

Dénomination attribuée à une balise html servant à introduire dans une page html le contenu d'une autre page web sans que l'internaute puisse en identifier la provenance. Elle permet notamment l'insertion de pages publicitaires à l'insu de l'internaute.

Injection SQL

On entend par injection SQL, l'exploitation d'une brèche dans la sécurité d'une base de données d'un site internet. Des informations sensibles peuvent ainsi être soustraites de manière frauduleuse. Cette méthode a pour objet la modification d'une requête SQL d'une page web en injectant du code SQL au moyen d'un formulaire. Cette attaque peut avoir pour effet la création, la suppression ou la modification d'enregistrement d'une base de donnée, de nouveaux comptes de connexion, le contournement de formulaires d'authentification ou encore l'exécution arbitraire de codes.

IP (Internet Protocol)

L'adresse IP est un numéro unique identifiant tout ordinateur connecté sur internet et autorisant sa communication dans un réseau. C'est le fournisseur d'accès qui est chargé d'assigner ce numéro à l'utilisateur.
La version 4 reste la plus employée. Elle est composée d'une série de nombres décimaux de 0 à 255 et espacés par des points.

IRC (Internet Relay Chat)

L'IRC ou discussion relayée par Internet est un protocole de communication prenant la forme d'une messagerie instantanée utilisé par les pirates depuis les années 90. On peut notamment y réaliser du transfert de fichiers.

KeyLogger (ou enregistrement de frappe)

Désigne un logiciel malveillant consistant à espionner les touches tapées sur un clavier d'ordinateur puis à les transmettre à un pirate à l'insu de l'utilisateur.
Cela concerne également les captures d'écran. Il peut être utilisé à des fins frauduleuses en s'accaparant des informations confidentielles relatives aux mots de passe et aux données financières. Il peut obtenir une certaine légitimité dans un contexte de surveillance informatique professionnel ou personnel.

LAG (ou latence)

Désigne le délai que prennent des données transmises dans un système pour parvenir à leur destinataire.
Une bonne latence est surtout appréciée dans le domaine des jeux en ligne ou des échanges vidéo.

Lamer (ou mauvais pirate)

Désigne le plus bas niveau dans le monde du hacking. Les lamers ne sont en mesure d'utiliser que des programmes impliquant le minimum de technique tels que le Nuking. Ils exploitent les actes de piratage développés par les pirates professionnels sont forcément y comprendre quoi que ce soit et soulignant dès lors leur manque de compétences.
Les maladresses de ces pirates plus qu'amateurs peuvent néanmoins conduire à la destruction des systèmes consultés.

Leaked

Désigne des informations usurpées à la suite d'une action de piratage.

LOIC (Low Orbit Ion cannon)

Ce logiciel signifiant "canon à ion en orbite basse", permet à un internaute amateur de contribuer à des attaques DDoS depuis son pc. Une multitude de requêtes sont ainsi transmises vers le site web ciblé entrainant la perturbation du serveur et à terme sa saturation. Pour lancer l'attaque, il suffit d'entrer l'adresse IP ou l'URL du site internet.
Cette application a connu son heure de gloire à travers le groupe hacktivisite Anonymous.

Mail bombing

Cette technique a pour objet d'envoyer une masse considérable de courriels accompagnés de fichiers volumineux sur le compte d'un utilisateur jusqu'à en provoquer la saturation.
La plupart du temps ces courriels espèrent aguicher les destinataires à travers notamment des communications publicitaires et promotionnelles.
Les conséquences peuvent en être la perte de la boîte mail visée, la diminution des performances du système ou encore l'infection des courriels par des virus.
Aussi, peut-il être nécessaire de posséder une seconde adresse mail et distinguer celle qui recevra des informations personnelles réduisant ainsi le risque de mail bombing.

MITM (Man-in-the-middle)

Le MITM ou " attaque de l'homme du milieu" désigne une attaque de piratage informatique consistant à capter des échanges de données cryptés entre deux systèmes de communication afin de les décoder. Le pirate ayant intercepté les messages transmis va être en mesure de les relayer à une partie en détournant l'identité de l'autre interlocuteur. Les données sont ainsi manipulées de façon frauduleuse.

Newbie (new beginner)

Désigne un utilisateur débutant dans l'univers du hacking qui aspire apprendre et évoluer rapidement.

Nuking

Cette technique a pour effet de déconnecter l'ordinateur d'un utilisateur en s'accaparant son adresse IP. Un signal "Out of Band" est alors transmis à la victime déconnectant ou rebootant (redémarrant) son pc.

OCLCTIC (Office Central de Lutte contre la Criminalité liée aux Technologies de l'information et de la Communication)

Créée en 2000, l'OCLCTIC réprime la criminalité informatique en France et intervient sous l'autorité de la "Direction Centrale de la Police Judiciaire" qui lui accorde un certain pouvoir d'investigation dans certaines conditions et pour une meilleure assistance technique.
Cette entité remplace la BRCI (Brigade centrale de la répression du crime informatique), désignant autrefois la police combattant la cybercriminalité au sein de l'hexagone.

OS (Operating system)

L'OS ou système d'exploitation est un logiciel pilotant les capacités d'une machine et recevant les commandes de l'utilisateur veillant ainsi à son bon fonctionnement.
Il est chargé de gérer la mémoire ainsi que les processeurs et les différents périphériques (la souris, l'écran, le disque dur ou encore le clavier) du système.
C'est cet ensemble de programmes qui est lancé en premier lors du démarrage de la machine.

Paquet

Un paquet correspond à un ensemble de données utilisé pour communiquer sur un réseau. Les fichiers transmis via ce réseau sont divisés en plusieurs paquets afin d'en faciliter la circulation depuis le périphérique source. Le paquet se divise en deux entités: les en-têtes et une partie des données. Lors de l'acheminement du paquet, les différents en-têtes sont ajoutés par segments à la partie correspondant aux données. Une fois arrivés à destination, les paquets peuvent être regroupés pour former un message complet. Les en-têtes auront été au préalable détruits dans leur ordre inverse d'ajout.
Peuvent être englobés dans un paquet, une requête de service, les

informations relatives au service ou des informations sur le mode de traitement de la requête.

PKI (Public Key Infrastructure)

Le système PKI ou " infrastructure à clé publique" est chargé d'assurer le respect des protocoles de sécurité sur Internet.

Le PKI procure à l'utilisateur un certificat numérique représentant son identité numérique et contenant une clé publique ainsi que des informations personnelles.
Il permet d'identifier les utilisateurs et de garantir la confidentialité et l'authentification des données communiquées en ligne. Le système PKI permet notamment la sécurité des achats sur internet via un système de chiffrement à clé publique.

Plugin

Le plugin ou " module d'extension" est un logiciel conçu pour compléter un logiciel hôte avec de nouvelles fonctionnalités. Le logiciel hôte fixe alors un standard d'échange d'informations auquel se conforment ses plugins.
À tout type de logiciel, ses plugins. Ainsi les plus connus relatifs aux navigateurs Web sont Java, Flash ou QuickTime.

Proxy

Désigne un serveur stockant localement les sites consultés par les internautes. Il joue ainsi le rôle d'intermédiaire entre un réseau local privé et un réseau internet.
La page demandée étant chargée depuis le cache proxy (et non plus depuis le site original), cela permet de booster les connections.

Ransomware

Désigne un virus dont l'objet est de chiffrer toutes les données d'un ordinateur afin de contraindre la victime à lui verser une rançon et ainsi récupérer ses données.

SQL

Le SQL ou " Structured Query Language" est un langage informatique standard utilisé afin de communiquer avec une base de données. Les

informations de celle-ci sont ainsi extraites puis mises à jour par les développeurs web. C'est sous la forme de commandes SQL que sont réalisées les requêtes. Celles-ci permettent la création de la base et des tables, la mise à jour des données, la modification de la structure de la table ou encore la gestion de droits d'utilisateurs de la base.

Spoofing (usurpation)

Cette technique de fraude a pour objet l'usurpation d'une identité électronique. Un utilisateur du réseau web s'empare d'une adresse IP se faisant alors passer pour une autre personne et transmettre des virus et autres spams. Cela permet de tromper les destinataires en les encourageant à ouvrir des courriels frauduleux et à communiquer des informations confidentielles.

URL (Universal Ressource Locator)

L'URL correspond à l'adresse d'un site internet. Celle-ci est saisie dans la barre de navigation afin d'afficher la page recherchée. Les internautes lui préfèrent les moteurs de recherche car apportant une meilleure simplicité via le champ de recherche.

Virus

Désigne un programme malveillant ayant pour objectif de se répandre à d'autres ordinateurs en bloquant, supprimant et détournant certaines données de la machine alors infectée. C'est notamment à travers les échanges de données numériques que le virus opère en corrompant courriels électroniques et pièces jointes.

VPN

Une VPN ou réseau privé virtuel, est un type de réseau établissant une connexion sécurisée et chiffrée entre l'utilisateur et le site internet visé. Ce mode de navigation ne laissant aucune trace, il autorise l'anonymat le plus complet. Cette technologie est notamment prisée des grandes entreprises, des organismes gouvernementaux, des universités et des grandes écoles où la confidentialité des informations est capitale.
À l'opposé, on retrouve les réseaux communs/classiques, ceux qu'on utilise tous les jours et qui peuvent permettre l'interception d'informations.

WAP (Wireless Application Protocol)

Désigne un protocole de communication conçu pour permettre à des appareils de taille réduite tels que les téléphones portables de se connecter sur internet. Le WAP simplifie les données affichées et prend en compte la taille réduite de l'écran des téléphones mobiles.
C'est l'ancêtre du GPRS qui est dorénavant utilisé.

Je vous remercie d’avoir lu ce livre. J’espère qu’il vous aura plu et qu’il vous aura appris un tas d’informations sur l’univers du hacking. Je vous dis à très vite… Benoît.

Your gateway to knowledge and culture. Accessible for everyone.