T3h Bo0k of P1r47eZ

to urduja for hacking my life

“we are anonymous
we are legion.
we do not forgive.
we do not forget.
expect us.”
anonymous

hack 001
ripping 002
linux 003
chaos computer club 004
hacker 005
malware 006
legion of doom 007
spamming 008
website defacement 009
hacktivismo 010
gnu 011
spoofing attack 012
the hacker manifesto 013
hacktivist 014
ingénierie sociale 015
freenet 016
phrack 017
white hat 018
packet sniffer 019
crypto-anarchisme 020
dos – denial of service attack 021
russian business network 022
security exploit 023
cracker 024
project chanology 025
swapper 026
cult of the dead cow 027
creative commons 028
phreaking 029
hacker con 030
ver 031
homebrew computer club 032
black hat 033
hacker ethic 034
phishing 035
rootkit 036
operation sundevil 037
jargon file 038
botnet 039
script kiddie 040
ascii art 041
1984 network liberty alliance 042
spyware 043
hacking 044
masters of deception 045
cheval de troie – trojan 046
logiciel open source 047
grey hat 048
jed – jam echelon day 049
leet 050
2600: the hacker quarterly 051
cypherpunk 052
vulnerability scanner 053
virus 054
hacktivism 055

001 hack

action qui consiste à détourner une machine, un code informatique ou un réseau de télécommunication afin d'en faire une utilisation différente de celle d'origine, d'en repousser les limites ou d'en contourner ses protections. la motivation peut être ludique, pécuniaire, politique ou l'accomplissement d'un exploit personnel.
le terme est apparu dans les années 60 et est attribué à certains laboratoires de recherche du mit, massachusetts institute of technology. il s'agissait d'un mot d'argot définissant une solution rapide élaborée ou bricolée pour résoudre un problème technique.
la pratique qui consiste a créer des hacks est le hacking [044] et les personnes qui l'exercent sont des hackers [005].

002 ripping

le ripping est une pratique de hacking [044] qui consiste à extraire un contenu audio ou vidéo d'un cd/dvd ou d'un stream internet, une diffusion en continu depuis un serveur, au moyen de logiciels prévus à cet effet. cette pratique est différente d'une simple copie de fichier car elle implique généralement que les fichiers extraits soient compressés et reformatés de sorte à être utilisable directement sur un ordinateur.
la compression permet l'allégement des fichiers ce qui rend leurs échanges au moyen d'internet plus facile. ainsi un dvd vidéo pesant en moyenne entre 4 et 7 gigaoctets et contenant nombre de fichiers vob sera compressé en un seul fichier avi pesant la plus part du temps 700 mégaoctets de sorte à tenir sur un cd-rom.
la copie privée, de sauvegarde, est pour l'instant autorisée dans la majorité des états, pourtant certains cd audio et presque tous les dvd vidéo sont protégés contre la copie. de plus, les grands groupes de distribution de contenus audio-visuels tendent à abolir ce droit, poussant ainsi leur clientèle à payer plusieurs fois pour le même contenu.

003 linux

linux est un système d'exploitation informatique pouvant être entre autres utilisé sur des téléphones portables, des ordinateurs personnels, des serveurs réseaux ou même des superordinateurs. la base a été créée par linus torvald en 1991 pour être ensuite continuellement enrichi par de nombreux contributeurs. c'est un système d'exploitation très apprécié des hackers [005] notamment pour ses

performances en termes de sécurité réseaux.
le système est une des références en terme de logiciels libres et de développements **open source** [047]. il se base sur le système d'exploitation **gnu** [011] mis en place par richard stallman en 1984. son code est donc complètement accessible et modifiable par tous. c'est pourquoi il en existe plusieurs versions, appelées distributions soit en éditeurs de texte, soit dotées d'une interface graphique.
il a été estimé que debian, une distribution de linux qui comporte plus de 283 millions de lignes de code source, aurait coûté 5.4 milliards de dollars s'il avait dû être développé par des moyens conventionnels.

004 chaos computer club

le chaos computer club, aussi nommé ccc, est l'une des plus grande organisation de **hackers** [005]. celle-ci, basée en allemagne et dans les pays germanophones, comprend environ 2000 membres.
le club se définit lui-même comme une communauté galactique d'êtres humains, quel que soit l'âge, le sexe, l'origine ethnique ou la position sociale, qui œuvre au travers des frontières pour la liberté d'information.
le ccc a été fondé à berlin en 1981 entre autres par wau holland. en 1984, le club se rend célèbre en **hackant** [044] la banque de hambourg et détournant ainsi 135'000 deutch marks. l'argent a été rendu le lendemain en présence de la presse. en 1989, le ccc refait parler de lui en étant indirectement impliqué dans le premier cas de cyber espionnage.
en 2001, le chaos computer club pour fêter ses 20 ans a créé une installation visuelle interactive en transformant la façade entière d'un immeuble à berlin en un écran d'ordinateur géant. en 2008, le ccc se procure et publie une empreinte digitale du ministre de l'intérieur allemand en protestation contre l'augmentation de l'utilisation de la biométrie.
le ccc organise chaque année le chaos communication congress, le plus grand **hacker con** [030] d'europe avec environ 4'500 participants. tous les quatre ans se tient le chaos communication camp, la version en extérieur du congrès.

005 hacker

individu qui effectue un **hack** [001], le hacker peut être de différentes types selon les raisons qui le poussent à **hacker** [044] et la façon

dont il procède.
les trois grandes familles sont black hat [033], grey hat [048] et white hat [018].
à celles-ci viennent s'ajouter des sous-familles telles que cracker [024], swapper [026], script kiddie [040], cypherpunk [052] et hacktivist [014].

006 malware

un malware, contraction des mots anglais malicious et software, est un logiciel destiné à nuire au système informatique dans lequel il est introduit sans l'autorisation de son possesseur, de son utilisateur ou de son administrateur. un malware se définit par les intentions malveillantes de son créateur plus que par sa fonction.
la famille des malwares comprend entre autres le virus [054], le ver [031], le cheval de troie [046], le rootkit [036] et le spyware [043].
d'après symantec, éditeur de logiciels spécialisé dans la sécurité informatique, la production, depuis le début de l'année 2008, de malware excéderait la production de logiciels conventionnels.
si dans les années 80 et 90, un malware était essentiellement utilisé pour faire des canulars ou du simple vandalisme, celui-ci est désormais employé à des fins autrement plus crapuleuses telles que la collecte de données personnelles, l'effacement de données ou encore la prise de contrôle d'un système informatique de façon illégale.

007 legion of doom

legion of doom, lod, est un groupe de phreakers [029] et de hackers [005] très influent, actif dès les années 80 et jusque dans les années 90. leur nom est une référence aux supervilains ennemis des superhéros du dessin animé challenge of the superfriends produit par dc comics.
le lod a été fondé par lex luthor après que celui-ci se soit séparé de son ancien groupe knights of shadow. le legion of doom a une branche spécialisée dans le hacking [044], le loh ou legion of hackers.
les membres les plus connus du lod sont chris goggans « erik bloodaxe », dave buchwald « bill from rnoc », patrick k. kroupa « lord digital », lloyd blankenship « the mentor » auteur du hacker manifesto [013], bruce fancher « Dead lord » et mark abene « phiber optik » qui en 1990 quitte le legion of doom pour rejoindre les masters of deception [045].

le groupe compte encore une dizaine de membres dont les noms et pseudonymes sont connus et une bonne vingtaine dont on ne connaît que les pseudonymes.
le legion of doom s'est opposé à ses rivaux, les masters of deception, mod, [045], lors du conflit appelé great hacker war, la grande guerre des hackers, qui dura de 1990 à 1991. bien que le legion of doom prétende le contraire, les masters of deception [045] auraient gagné la guerre ce qui aurait poussé chris goggans, frustré par sa défaite, à révéler des informations concernant les mod [045] au fbi.

008 spamming

le spamming est la pratique qui consiste à envoyer un message non sollicité, un spam, un très grand nombre de fois et/ou à un très grand nombre de personnes. la forme la plus répandue de spamming se fait à travers l'email, mais le spam se diffuse aussi sur les messageries instantanées, les chat rooms, les forums, les blogs, les sites de partages de vidéos et les téléphones portables.
le contenu d'un spam peut être religieux ou politique, mais il s'agit généralement d'un contenu commercial proposant des services financiers douteux, des contenus pornographiques ou des médicaments normalement impossibles à obtenir sans ordonnance. le spamming peut aussi servir à véhiculer un cheval de troie [046], un virus [054], un ver [031], un spyware [043] ou un malware [006].
le nom spam provient d'une marque de viande en boîte du même nom, réputée pour son mauvais goût, et d'un sketch des monty pythons, un groupe de comiques anglais, durant lequel le mot spam est omniprésent.
on estime la quantité de spams envoyés dans le monde par jour à 100 milliards, un chiffre qui augmente chaque année. malgré la qualité des filtres anti-spams des services email et le fait que nombre d'adresses utilisées par les spammers ne soient plus valides, plus de 80% des emails envoyés sont des spams.

009 website defacement

un website defacement consiste à effacer la page d'accueil d'un site web sans l'autorisation de son possesseur ou de la personne qui le gère pour la remplacer par une autre de sa propre création.
un message est généralement laissé par le hacker [005] mentionnant son pseudonyme et des dédicaces pour ses amis ou les membres de son collectif. parfois, l'attaquant se moque de l'administra-

teur système pour ne pas avoir réussi à maintenir la sécurité de son serveur.
la plupart du temps le website defacement est inoffensif, mais il peut aussi servir de distraction pour une autre attaque beaucoup plus dangereuse et insidieuse telle qu'uploader un malware [006].
un website defacement très populaire est celui du site de sco, une compagnie prétendant que linux [003] utilisait du code leur appartenant. peu de temps après l'avoir annoncé comme un vol, un texte de même apparence que la ligne graphique de sco a été placé sur leur page d'accueil. celui-ci disait « nous possédons tout votre code, payez nous tout votre argent ».

010 hacktivismo

hacktivismo est un groupe d'hacktivists [014] fondé en 1999 par oxblood ruffin. celui-ci fait partie de cdc communication, une organisation de hackers [005], au côté de cult of the dead cow [027] et ninja strike force.
hacktivismo cherche à faire valoir et à faire respecter les articles 19 de la déclaration universelle des droits de l'homme ainsi que ceux du pacte international relatif aux droits civils et politiques sur internet. ceux-ci concernent la liberté d'opinion et d'expression et le libre accès à l'information et aux media.
the hacktivismo declaration, postée sur leur site web, recense une liste d'évènements qui bafouent ces droits, puis explique leurs intentions. les sources de ces évènements sont des rapports de reporters sans frontière.
dans ce sens, oxblood rufifn s'oppose fortement au website defacement [009] et au denial-of-service attack [021] perpétrés par d'autres hacktivists [014].
hacktivismo produit différents logiciels, tels camera/shy, the six/four system, scatter chat et xerobank browser, dont les applications sont, entre autres, le cryptage et le décryptage de communications et de contenus numériques et le contournement des filtres de censure internet.

011 gnu

gnu est un système d'exploitation informatique composé entièrement de logiciels libres. son nom est un acronyme récursif pour gnu's not unix, gnu n'est pas unix, un système d'exploitation majeur mais payant. gnu est très proche d'unix, mais se différencie de ce-

lui-ci, car il est un système libre et ne contient aucune ligne de code provenant d'unix.
le projet gnu est initialisé en 1984 par richard stallman. lorsque celui-ci quitte son emploi au mit, massachusetts institute of technology, pour assurer l'indépendance de son système d'exploitation, son but est de créer un système d'exploitation complètement libre. en 1989, richard stallman écrit la gnu gpl, gnu general public license, licence de logiciel libre créé à l'origine pour gnu mais désormais appliquée à de nombreux logiciels.
si la plupart des éléments du système d'exploitation sont prêts, il lui manque encore l'essentiel, le gnu hurd, son noyau officiel encore inachevé. c'est pourquoi la majorité de ses utilisateurs emploient le noyau de linux [003] parfaitement compatible. à noter qu'en 2004, l'unesco a déclaré gnu comme trésor du monde.

012 spoofing attack

un spoofing attack est une situation dans laquelle une personne se fait passer pour une autre en falsifiant des données de sorte à obtenir l'accès à certaines informations. il existe plusieurs formes de spoofing tels que le man-in-the-middle attack, le phishing [035], le file-sharing network spoofing, le caller id spoofing et l'email address spoofing.
le man-in-the-middle attack est une technique qui consiste à faire croire à x que l'on est y et à y que l'on est x en interceptant les communications émises par les deux parties, puis en prenant la place de l'un ou de l'autre dans la communication.
le phishing [035] est une technique qui consiste à se faire passer pour une institution connue et digne de confiance en imitant sa ligne graphique lors d'une communication numérique de sorte à obtenir des informations sensibles.
le file-sharing network spoofing est une pollution émise par les majors de l'industrie du disque qui consiste à inonder les réseaux de partage de musique avec des fichiers portant le nom de morceaux populaires mais qui ne contiennent en réalité que des messages contre le téléchargement illégal.
le caller id spoofing et l'email address spoofing fonctionnent sur le même principe qui consiste à usurper le numéro de téléphone ou l'adresse email d'un tiers de façon à rendre sa communication légitime ou à ne pas dévoiler la source réelle de la communication.

013 the hacker manifesto

the conscience of a hacker aussi connu sous le nom de the hacker manifesto est un court essai rédigé en 1986 par un hacker [005] membre de legion of doom [007] dont le pseudonyme est the mentor et dont le nom officiel est lloyd blankenship. le texte est écrit après l'arrestation de son auteur et est publié pour la première fois dans le magazine électronique phrack [017], volume 1, publication 7, fichier 3 sur 10.

il est considéré comme une des bases de la culture hacker [005] et révèle la psychologie originelle de ceux-ci. le manifeste déclare que le hacker [005] développe cette pratique parce que c'est une façon d'apprendre et parce qu'il est souvent frustré par les limitations de la société standard.

de nos jours, le manifeste reste une ligne de conduite pour le hacker [005]. il sert de base éthique à la pratique du hacking [044], démontrant qu'il y a une raison à celle-ci qui dépasse le désir personnel et égoïste et que la technologie doit être utilisée pour étendre nos horizons et garder le monde libre.

le hacker manifesto est cité dans le film hackers de 1995, mais les protagonistes le lisent dans le magazine 2600: the hacker quarterly [051], alors qu'il a été publié à l'origine dans phrack [017], un magazine électronique.

014 hacktivist

un hacktivist, contraction des mots hack [001] et activist, se sert des outils informatiques et des réseaux de télécommunication de façon non violente, mais souvent illégale pour promouvoir des idées politiques.

il se sert de techniques de hacking [044] pour effacer un site web, website defacement [009], rediriger le visiteur vers une autre page, commettre des attaques dos, denial-of-service attacks [021], voler des informations, créer des parodies de sites web ou organiser des sit-ins virtuels qui consistent à ce qu'un grand nombre de personnes se connectent en même temps à un serveur de sorte à le saturer.

certains hacktivists désapprouvent le website defacement [009] et le denial-of-service attacks [021] affirmant que ces méthodes contredisent le principe de liberté d'expression, gaspillent des ressources et que cela pourrait mener à une guerre de denial-of-service attacks [021] que personne ne pourrait gagner.

les groupes d'hacktivists les plus connus sont hacktivismo [010], branche activiste du groupe de hackers [005] cult of the dead cow

[027], et le 1984 network liberty alliance [042].

015 ingénierie sociale

l'ingénierie sociale est la pratique qui consiste à tromper son interlocuteur en exploitant sa confiance, son ignorance ou sa naïveté afin d'obtenir une information confidentielle. partant du principe qu'il est plus facile d'obtenir des informations d'une personne que d'une machine, le hacker [005] a ajouté cette technique humaine à sa pratique de l'informatique.
il existe plusieurs variantes, mais il s'agit en général de posséder un certain nombre d'informations de base de sorte à se positionner d'une manière bien précise face à son interlocuteur. se faire passer pour un employé de la maintenance informatique ou pour un supérieur hiérarchique haut placé par exemple permettra d'obtenir des informations différentes.
le maître incontesté de l'ingénierie sociale est kevin mitnick qui, malgré ses indéniables compétences en informatique, en avait fait sa technique de prédilection.

016 freenet

freenet est un logiciel donnant accès à un réseau de peer to peer, pair à pair en français, dont le but est de proposer une liberté d'expression totale en offrant une protection de l'anonymat maximale.
le projet, conçu à l'origine par ian clarke, est en développement depuis l'an 2000. il n'existe encore à l'heure actuelle pas de version 1.0 et la version disponible la plus récente est la 0.7 parfaitement utilisable et publiée sous licence gnu [011] general public license.
la spécificité de freenet contrairement aux autres réseaux de peer to peer est qu'il scinde et encode les fichiers hébergés par ses utilisateurs. de cette manière même l'utilisateur n'a pas idée des fragments de fichiers qu'il héberge. quand un utilisateur veut télécharger un fichier, freenet va aller chercher les différents fragments chez de nombreux utilisateurs, les décoder et restituer le fichier original.

017 phrack

phrack est un magazine électronique ouvert à la contribution de tous les hackers [005] publié pour la première fois en novembre 1985. le magazine couvre de nombreux sujets relatifs au hacking [044] tel le phreaking [029], le cracking [024] ou la cryptographie, mais

aussi parfois en lien avec une certaine forme d'anarchie, comme le crypto-anarchisme [020].
le nom phrack provient de la contraction de phreak [029] et de hack [001]. la majorité des 30 premières éditions sont publiées par les fondateurs du magazine, taran king et knight lightning. phrack compte désormais un grand nombre de contributeurs plus ou moins réguliers, dont erik bloodaxe et the mentor, deux anciens membres de legion of doom [007].
the mentor a notamment publié son hacker manifesto [013] dans l'édition de phrack, volume 1, publication 7, fichier 3 sur 10.
les publications se font de manière irrégulière. celles-ci sont regroupées en volume et comportent toutes un certain nombre de fichiers textes appelés philes. la plupart des publications comprennent certaines rubriques récurrentes telle prophile, la présentation d'un hacker [005] influent, loopback, les réponses aux emails les plus originaux ou les plus stupides, phrack world news, des rapports concernant la contre-culture et international scene, des témoignages de hackers [005] provenant de différents pays.
il est intéressant de voir que phrack publie dans sa rubrique stat, en plus du top 10 des articles les plus lus, le top 10 des agences gouvernementales ainsi que le top 10 des agences militaires ayant le plus consulté le site.

018 white hat

le white hat est un hacker [005] qui respecte la loi. il travaille, à travers des entreprises de sécurité informatique et réseau, généralement pour les institutions économiques et politiques en place.
son travail consiste à chercher les failles de sécurité d'un système afin de le rendre plus performant et de le prévenir de toute attaque.
il prétend être le seul a respecter l'éthique du hacker [034] et méprise généralement le black hat [033]. il appelle celui-ci cracker [024] estimant qu'il n'est pas un hacker [005].
néanmoins, certains white hats sont à l'origine d'importantes alternatives au système en place, tels que les systèmes d'exploitations libres linux [003] et gnu [011], les logiciels open source [047], ou les licences creative commons [028].
les white hats célèbres sont eric corley, aka emmanuel goldstein, fondateur de 2600: the hacker quarterly [051], gordon lyon, aka fyodor vaskovich, expert en sécurité auteurs de nombreux livres, tsutomu shimomura qui a aidé le fbi a arrêté kevin mitnick, linus torvald créateur de linux [003], richard stallman à l'origine de gnu

[011] et eric s. raymond détenteur actuel du jargon file [038]. un des plus célèbres groupes de white hats est le homebrew computer club [032].

019 packet sniffer

le packet sniffer est un malware [006] ou un matériel informatique qui permet d'intercepter et de consigner le trafic effectué sur un réseau numérique. au fur et à mesure que les données transitent, le sniffer capture tous les paquets du flux, les décode et les analyse.
cela peut se faire dans le but de contrôler les flux d'un réseau pour s'assurer de son bon fonctionnement, mais aussi pour intercepter mots de passe ou autres données sensibles alors que les paquets de données sont en transit.

020 crypto-anarchisme

le crypto-anarchisme est une idéologie qui prône l'usage de logiciels de cryptographie asymétrique, appelée aussi cryptographie à clé publique, dans les communications numériques afin de protéger la liberté d'expression et l'intégrité des données privées. ses idées et ses effets ont été exposés par timothy c. may dans cyphernomicon, un document publié dans les mailing listes cypherpunks [052].
l'emploi de tels outils rend l'identification et la localisation de l'utilisateur impossible à prouver et le contenu de la communication impossible à déterminer. on peut considérer ce réseau anonyme, appelé le cipherspace, comme un espace sans loi, cependant il est malgré tout soumis à ses propres règles.
une des principales motivations du crypto-anarchisme est de se défendre contre la surveillance intrusive opérée sur les réseaux informatiques par certaines sociétés commerciales et par les agences de sécurité gouvernementales. une autre motivation importante est d'échapper à la censure et d'offrir une liberté d'expression totale grâce à l'anonymat, ce qui peut entre autres aider l'opposition politique à diffuser des informations sous un régime oppressif.
du fait de ses spécificités, le crypto-anarchisme est souvent critiqué parce qu'il facilite d'une part l'échange de fichiers protégés par des droits d'auteur, et d'autre part l'accès à de grandes quantités de pornographie enfantine. on peut aussi imaginer que le cipherspace est utilisé pour coordonner des actes de sabotage ou de terrorisme.
le crypto-anarchiste est conscient que son système peut être détourné à des fins criminelles, mais affirme que le criminel communi-

que déjà par d'autres voies anonymes.
il existe des banques anonymes opérant dans le cipherspace telles ecache toujours en activité ou digital monetary trust et yodelbank toutes deux désormais inactives. ces banques ne sont enregistrées dans aucun pays et les identités de leurs opérateurs sont parfaitement inconnues.

021 dos – denial of service attack

un dos, denial of service attack, est une tentative visant à rendre les ressources d'un système informatique inaccessible pour ses utilisateurs. il s'agit généralement d'une attaque dirigée vers un site web ou un service internet pour empêcher celui-ci de fonctionner correctement pendant une durée temporaire ou indéfinie.
un dos peut se manifester de différentes manières : des performances réseaux inhabituellement lentes, l'impossibilité d'accéder à un site web bien précis, l'impossibilité d'accéder à n'importe quel site web ou une augmentation exceptionnelle du nombre de spams [008] reçus, l'attaque est alors appelée un mail-bomb.
les cinq attaques de base d'un dos sont : l'utilisation excessive des ressources informatiques telles que la bande passante, l'espace disque ou le processeur, la perturbation des informations de configuration, la perturbation de l'état d'information, la perturbation des composants physiques du réseau et l'obstruction de la communication entre l'utilisateur et le serveur victime de l'attaque.
un dos peut être effectué depuis plusieurs ordinateurs à la fois, à travers un botnet [039], on l'appelle alors ddos attack, distributed denial of service attack. le hacker [005] introduit un malware [006] dans un très grand nombre de systèmes ce qui lui permet ensuite de lancer une attaque depuis toutes ces machines en même temps.

022 russian business network

le russian business network, rbn, est une des plus puissantes organisations de cyber crime basée physiquement à saint-petersbourg. on la dit être la pire parmi les pires. spécialisée entre autres dans le phishing [035], le vol et la revente d'identités, l'organisation est aussi connue pour héberger toutes sortes de sites crapuleux diffusant pornographie enfantine, spams [008] et malwares [006].
le rbn est le créateur du logiciel mpack, un malware [006] vendu comme un logiciel commercial, et l'opérateur supposé du storm botnet, un botnet [039] qui comprendrait 250'000 ordinateurs zombies

pour les plus optimistes et 50 millions pour les plus pessimistes. le russian business network vend ainsi des services de ddos attack [021] et des locations de segments de son botnet [039].
l'organisation est difficile à tracer car elle n'est enregistrée nulle part légalement et ses différents noms de domaine sont enregistrés anonymement. de plus, ses communications et autres transactions sont cryptées. et surtout, elle est connue pour attaquer quiconque essayant de remonter à sa source ou de s'opposer à ses activités.
le rbn existe aussi à travers de nombreuses autres compagnies sans base géographique. on suppose que flyman, le fondateur et leader de l'organisation, serait allié à un puissant homme politique russe. il serait ainsi possible que le rbn soit en partie responsable de l'attaque cyber terroriste dont a été victime l'estonie en mai 2007.

023 security exploit

un security exploit est une suite de lignes de code, de données ou de commandes préparée de sorte à exploiter un bug ou une faille d'un logiciel informatique ou d'une partie matérielle d'un ordinateur. cela inclut souvent le fait de prendre contrôle d'un ordinateur ou d'un serveur informatique de façon illégale.
le security exploit peut être de différentes natures selon qu'il soit exécuté de façon distante ou locale et selon l'action même à travers laquelle il se développe. il permet d'accéder généralement directement à un statut de super-utilisateur, qui a toutes les autorisations, mais il se peut aussi que le security exploit ne donne accès qu'à un bas niveau d'autorisation, auquel cas, l'utilisateur devra escalader les privilèges les uns après les autres pour arriver jusqu'à la racine, root.
un security exploit ne profite normalement que d'une seule faille. en principe, une fois découverte, cette faille est publiée et réparée au moyen d'un patch qui la rend obsolète. c'est pour cette raison que certains black hats [033] ne publient pas leurs security exploits de sorte à pouvoir en profiter plus longtemps.

024 cracker

le white hat [018] qui ne considère pas le black hat [033] propre à partager le nom de hacker [005] avec lui appelle celui-ci cracker.
le cracker, tout comme le black hat [033], travaille de manière illicite, mais sa pratique se spécialise généralement dans la modification de logiciels de sorte à en casser les protections, celles-ci pouvant se

manifester sous forme de cryptage anti-copie, de version d'essai limitée dans le temps, de numéro de série, de clé matérielle ou de demande d'insertion du cd /dvd original.
ses aptitudes en programmation lui permettent, en accédant au code source, de changer l'exécution du logiciel de sorte que lorsque celui-ci arrive à la protection, il est redirigé vers un autre script ou simplement l'évite et continue l'exécution normalement.
cette pratique, après diffusion, permet l'utilisation de logiciels dit crackés par tout un chacun sans avoir à payer pour posséder l'original et son droit d'exploitation. l'utilisation de tels logiciels est totalement interdite par la loi.

025 project chanology

le project chanology est un raid mené par les anonymous contre l'église de scientologie. les anons, ou anonymous, sont à l'origine une communauté de hackers [005], mais à travers le projet chanology de nombreuses personnes de tous horizons ont rejoints leurs rangs. le nom anonymous définit à la fois l'individu et le groupe.
le projet a démarré publiquement le 21 janvier 2008, lorsque les anonymous ont posté une vidéo sur le site de partage youtube déclarant la guerre à l'église de scientologie. la raison à l'origine de cette déclaration est la censure exercée par l'église sur les sites web youtube et gawker.com. on pouvait y voir une vidéo dans laquelle l'acteur tom cruise fait l'éloge de l'église de scientologie.
les anonymous perpétuent alors de nombreuses attaques ddos [021] contre les sites web de l'église de scientologie et arrivent effectivement à les mettre hors ligne, le temps qu'elle déplace tous ses sites chez un hébergeur spécialisé dans la sécurité informatique.
les anonymous procèdent aussi à des google bombs, technique qui leur permet de faire apparaître le site officiel de l'église de scientologie en tête des résultats sur le moteur de recherche google pour les requêtes dangerous cult et brainwashing cult, secte dangereuse et secte à lavage de cerveaux.
au même moment, les anonymous organisent des manifestations devant les églises de scientologie partout dans le monde incitant les participants à porter un masque de guy fawes personnage historique et héros anarchiste de la bande dessinée et du film v for vandetta.
même si beaucoup apprécient leur action contre l'église de scientologie, les anonymous ont été vivement critiqués pour leurs méthodes illégales de hacking [044] et sembleraient désormais se concentrer

sur les manifestations et l'emploi de méthodes en accord avec la législation.

026 swapper

le swapper a pour but d'échanger un maximum de warez, contenus informatiques piratés tels que logiciels (appz), jeux (gamez), musique (mp3z), films (ripz), etc, sans pour autant forcément s'en servir lui-même. il est à la fois collectionneur et distributeur, mais ne hacke [044] pas à proprement parler.
ces échanges peuvent se faire sur des supports matériels comme cd-rom ou dvd, mais le swapper se sert surtout d'internet. il utilise les réseaux de peer-to-peer, gnutella, edonkey ou bit torrent par exemple, mais aussi des sites internet exclusivement dédiés aux partage de contenus piratés ou des boardz, forums sur lesquels on s'échange les liens vers les warez.

027 cult of the dead cow

cult of the dead cow, cdc, est une organisation de hackers [005] créée par grandmaster ratte', franken gibe et sid vicious en 1984 au texas.
en 1990, drunkfux, un membre du cult of the dead cow, met en place le hohocon, il s'agit d'un des premiers hacker con [030], les assemblées de hackers [005], dont la particularité a été d'inviter des journalistes et des représentants des forces de l'ordre. il y a eu cinq éditions annuelles de hohocon au texas.
le cult of the dead cow fait partie du cdc communications, une organisation qui comprend deux autres groupes, ninja strike force et hacktivismo [010]. ninja strike force consiste en un groupe d'élite qui se consacre à réaliser les but du cdc. hacktivismo [010] est une branche hacktivist [014] de l'organisation.
depuis 1996, le groupe se consacre aussi à l'hacktivism [055]. le cdc a colaboré à la fin des années 90 avec un groupe de dissidents chinois appelé les hong kong blondes. leur but était de désactiver les filtres internet chinois de sorte que la population ait accès à un internet non censuré.
cult of the dead produit aussi des logiciels dédiés à la sécurité informatique dont le plus célèbre est back orifice. celui-ci permet de prendre le contrôle à distance d'un ordinateur fonctionnant sous microsoft windows. il tient son nom d'un autre logiciel microsoft appelé back office server.

028 creative commons

creative commons est une organisation sans but lucratif, fondée en 2001 par lawrence lessig, qui s'applique à rendre une création facile à partager et à réutiliser. l'organisation a établi un certain nombre de licences de droits d'auteurs en 2002 inspirées de l'open source [047] et des logiciels libres.

les licences s'articulent à travers la combinaison de quatre conditions : attribution (by), noncommercial (nc), no derivated works (nd) et sharealike (sa). attribution autorise la duplication, la distribution, la présentation et la création de dérivés. noncommercial autorise la duplication, la distribution, la présentation et la création de dérivés, mais uniquement dans un but non commercial. no derivate works ou noderivs autorise la duplication, la distribution et la présentation, mais interdit la création de dérivés. sharealike n'autorise la distribution de dérivés que si la même licence leur est attribuée.

la combinaison de ces quatre conditions donne 16 possibilités. cinq ne sont pas applicables car leurs conditions seraient contradictoires et cinq sont inutilisées car n'incluant pas attribution. il reste six licences : attribution, attribution + noncommercial, attribution + noderivs, attribution + sharealike, attribution + noncommercial + noderivs, attribution + noncommercial + sharealike.

029 phreaking

le phreaking, contraction des mots phone et freak, est une pratique qui consiste à se servir de différentes méthodes de sorte à manipuler, explorer ou utiliser de façon frauduleuse un système de communication téléphonique.

on doit le premier acte reconnu de phreaking à un enfant aveugle de huit ans, joseph engressia, en 1957. ayant l'oreille absolue, il s'est rendu compte qu'en sifflant le 4e mi au-dessus d'un do, soit une fréquence de 2600 hz, il pouvait arrêter un téléphone d'enregistrer.

le phreaking a été exposé au public en 1971, lorsque le magazine esquire a publié un article, secrets of the little blue box, boîtier électronique permettant de simuler les fréquences produites par un opérateur téléphonique, décrivant les exploits de joseph engressia, devenu joybubbles, et john draper, capitain crunch. celui-ci est un des phreakers les plus connus pour avoir utilisé un sifflet en plastique offert dans les boîte de céréale cap'n crunch qui produisait la fréquence de 2600 hz.

durant les années 80 et la révolution des ordinateurs personnels, le phreaking s'est popularisé à travers les bulletin board systems,

serveurs accessibles par modem permettant l'échange de fichiers ou d'informations. cela a donné lieu à la création de la sous-culture h/p (hacking/phreaking) dont les groupes les plus célèbres étaient masters of deception [045] et legion of doom [007].
de nos jours, peu de gens pratiquent encore le phreaking. l'internet offre des possibilités d'explorations et de fraudes beaucoup plus étendues tout en présentant des risques moindres.

030 hacker con

hacker con, de hacker convention en anglais, est un terme désignant les grands rassemblements de hackers [005] de part le monde. ces rassemblements peuvent être de différents types selon l'association qui la gère. un hacker con peut être transversale et intéresser aussi bien le black hat [033], le grey hat [048] ou le white hat [018], ou alors être destinés à un public bien précis.
les sujets traités dépendent évidemment du type de rassemblement, mais s'articulent généralement autour de la sécurité informatique, des nouvelles technologies, de la liberté d'expression et du libre accès à l'information. certains proposent des concours ou des actions collaboratives, tels les hackatons.
les hacker con les plus connus sont summer con, le plus vieux rassemblement de hackers [005] établit par phrack [017] hohocon, établi par le cult of the dead cow [027], h.o.p.e., mis en place par 2600: the hacker quarterly [051], le chaos computer congress, organisé par le chaos computer club [004] et def con, le plus grand des hacker con.

031 ver

un ver informatique, worm en anglais, est un logiciel qui se duplique et infecte un système informatique sans l'autorisation de son possesseur, de son utilisateur ou de son administrateur. contrairement à un virus [054], il n'a pas besoin d'hôte pour se propager et utilise de lui-même les ressources et les connexions réseaux disponibles.
outre sa propagation, le but du ver peut être de diverses natures, mais il est généralement un malware [006]. il peut notamment effacer des données, endommager un système, récolter des informations, servir de backdoor, porte de derrière permettant un accès caché, ou servir à travers un botnet [039] à perpétrer un ddos attack [021].
le ver le plus connu est certainement le ver iloveyou. celui-ci est parti des philippines le 4 mai 2000 et s'est répandu dans le monde entier

en un jour, infectant 10% des ordinateurs connectés à internet. il consistait en un email dont l'intitulé était iloveyou et une pièce jointe nommée love-letter-for-you.txt.vbs. une fois la pièce jointe ouverte, le vers remplaçait des fichiers entiers par son propre code et se propageait en envoyant un email similaire à tout le carnet d'adresses de la victime. les dégâts ont été estimés à 5.5 milliards de dollars.

032 homebrew computer club

le homebrew computer club est un groupe informel de passionnés d'informatique qui s'est réuni dans la silicon valley en californie de 1975 à 1977 pour s'échanger des pièces détachées, des circuits imprimés et des informations afin de construire eux-mêmes des ordinateurs.
le groupe a été créé par gordon french et fred moore dans l'idée d'avoir un forum ouvert pour rendre les ordinateurs plus accessibles.
le homebrew computer club éditait une newsletter qui a été à l'origine de l'idée de l'ordinateur personnel.
le club s'est rendu célèbre pour avoir vu naître nombre de **hackers** [005] importants et plusieurs fondateurs de compagnies informatiques dont notamment steve jobs et steve wozniak fondateur de apple computer.

033 black hat

le black hat est la frange criminelle du **hacking** [044]. il travaille de façon illégale et ne partage généralement pas ses techniques afin de pouvoir mieux en profiter. par conséquent, le black hat est la cible d'opérations de répression comme l'**operation sundevil** [037] en 1990
si le jeu et l'accomplissement d'un exploit sont ses principales motivations, il se peut que le black hat **hacke** [044] aussi pour de l'argent.
il travaille à son compte ou peut être engagé par des associations de crime organisé dans le but de détourner des fonds, voler des identités ou usurper des cartes de crédits.
comme le **grey hat** [048], lorsque le black hat oeuvre pour des raisons politiques, il est alors **hacktivist** [014].
il existe de nombreux black hats célèbres tels marc abene aka phiber optik, membre de **legion of doom** [007] d'abord, puis des **masters of deception** [045], john draper, aka captain crunch, un des premiers **phreakers** [029], nahshon even-chaim, aka phoenix, qui

s'en est pris au système informatique de l'us défense and nuclear research, markus hess qui a **hacké** [044] les sites militaires américains pour le kgb, jonathan james, aka c0mrade, qui a téléchargé des logiciels de l'international space station estimé à 1.7 million de dollars, adrian lamo qui s'est introduit dans le réseau du new york times, vladimir levin qui a dérobé 10.7 millions de dollars à la citybank, kevin mitnick connu pour être un maître de l'**ingénierie sociale** [015], robert tappan morris qui a créé le premier **ver** [031], craig neidorf, aka knight lightning, qui est le cofondateur de **phrack** [017] et kevin poulsen, aka dark dante, devenu depuis rédacteur en chef de wired news, la version électronique de wired magazine.
le **white hat** [018], estimant que le black hat galvaude le terme **hacker** [005], appelle celui-ci **cracker** [024].

034 hacker ethic

le hacker ethic ou éthique du hacker en français se réfère aux valeurs et la philosophie appliquées par certains **hackers** [005]. elle provient en grande partie de la philosophie des premiers **hackers** [005] du mit, massachusets institute of technology. le terme hacker ethic est attribué au journaliste steven levy tel qu'il le définit dans son livre hackers: heroes of the computer revolution écrit en 1984.
steven levy énonce dès la préface de hackers: heroes of the computer revolution les principe de base de cette éthique, à savoir : le partage, l'ouverture, la décentralisation, l'accès libre aux ordinateurs et l'amélioration de notre monde. il les développe dans le chapitre 2 et ajoute que toute information devrait être libre, qu'il faut se méfier des autorités, qu'un **hacker** [005] ne doit être jugé que selon ses **hacks** [001] et non selon ses diplômes, son âge, sa race ou sa position, que l'on peut créer de l'art et quelque chose de beau avec un ordinateur et qu'un ordinateur peut changer la vie pour le mieux.
il existe aussi un livre intitulé the hacker ethic écrit en 2001 par le philosophe finlandais pekka himanen. il oppose l'éthique hacker à l'éthique protestante du travail à travers trois pôles : l'éthique du travail, l'éthique de l'argent et l'éthique du réseau.

035 phishing

le phishing, hameçonnage en français, est le résultat d'une certaine forme d'**ingénierie sociale** [015] et d'une certaine forme de **spoofing attack** [012]. cette pratique consiste à acquérir des informations sensibles telles que nom d'utilisateur, mot de passe ou numéro de

carte de crédit en se faisant passer pour une institution digne de confiance à travers une communication numérique.
le nom phishing, dont la première utilisation remonte à 1996, est une variante du mot anglais fishing pêcher. le ph proviendrait soit de l'influence du phreaking [029], soit du leet [050] ou l'utilisation de ph comme substitutif à f est courante, soit de l'expression password harvesting fishing, la pêche au mot de passe.
le phishing est généralement propagé par un email imitant à la perfection le nom et la ligne graphique d'une société internet bien connue, d'une banque ou d'un site gouvernemental. le message invite l'utilisateur à se rendre sur une page où il est amené à rentrer des informations personnelles qu'il ne communiquerait pas autrement.
le phishing peut être réalisé par téléphone, il s'agit alors de vishing (voice phishing). un message invite la victime à appeler un certain numéro (appartenant au phisher) prétextant un souci avec son compte en banque par exemple. une fois le numéro atteint, il lui est demandé de composer son numéro de compte et son code pin ce qui permet au phisher de les récupérer.
le phishing a été reconnu en 2004 comme part industrialisée de l'économie du crime. en 2006, il a été établi que plus de la moitié des cas de phishing avaient été perpétré par des groupes opérant à travers le russian business network [022]. les pertes sont estimées à plus de 2 milliard de dollars par année uniquement pour l'économie américaine.

036 rootkit

un rootkit était à l'origine une application légale permettant en cas d'urgence ou lors de non-réponse d'un système informatique d'en prendre ainsi le contrôle pour pouvoir l'analyser et le réparer. désormais, il s'agit essentiellement d'un malware [006] utilisé dans la piraterie informatique.
celui-ci donne la possibilité d'accéder au contrôle complet, root ou administrator selon les systèmes d'exploitations, d'un système informatique sans l'autorisation du propriétaire ni de la personne qui le gère ou l'utilise et ceci sans se faire détecter.
le rootkit contourne les mécanismes de sécurité du système d'exploitation en place de différentes manières, parfois en modifiant directement le code source. il dissimule non seulement son installation, sa présence et son activité, mais aussi ses connexions réseaux. comme il est directement installé à la source du système d'exploita-

tion, il est quasiment impossible de l'enlever et il vaut généralement mieux sauvegarder les données, formater le disque dur et réinstaller le système.

037 operation sundevil

l'opération sundevil est la plus connue et la plus importante des nombreuses opérations menées par les services secrets américains contre des hackers [005] durant les années 90.
elle a été menée conjointement par les forces spéciales de la police de chicago et par le bureau contre le crime organisé de l'arizona dans les villes de austin, plano, détroit, los angeles, miami, new york, newark, phoenix, pittsburg, richmond, tucson, san diego, san jose et san fancisco les 7,8 et 9 mai 1990.
l'opération a visé essentiellement les bulletin board systems, serveurs accessibles par modem permettant l'échange de fichiers ou d'informations, dans le but de s'en prendre aux vols de cartes de crédits et à la fraude téléphonique, mais n'a conduit qu'à l'arrestation de quatre hackers [005].

038 jargon file

le jargon file est un dictionnaire composé des expressions et de l'argot utilisé par la communauté hacker [005].
la première version a été écrite en 1975 par raphael finkel au stanford ai labs, le laboratoire de recherche sur l'intelligence artificielle de l'université de stanford. il la nomme aiword.rfdoc. en 1976, mark crispin voit une annonce concernant le fichier aiword.rfdoc sur l'ordinateur du stanford ai labs et le télécharge pour le mit, massachusetts institute of technology. celui-ci, aidé de guy steel, le complète et l'enrichit grandement.
en 1981, un hacker [005] du nom de charles spurgeon publie une grande partie du jargon file dans un magazine appelé coevolution quarterly. c'est la première publication papier du file. en 1983, guy steel, avec la participation des auteurs originaux et entre autre de richard stallman, créateur du projet gnu [011], publie la première version papier complète du jargon file aux éditions harper & row sous le nom de the hacker's dictionary.
durant le reste des années 80, le file n'a plus évolué pour différentes raisons, notamment à cause de la réduction de budget imposé aux laboratoires de recherches et de la disparition du stanford ai labs. en 1990, une nouvelle révision est entamée. en accord avec les auteurs

de la version 1, 80% du texte original est gardé et le champ est élargit aux différents systèmes sur lesquels le hacker [005] agit.
désormais, c'est eric s. raymond qui conserve le jargon file. il en a publié la troisième version sous le nom de the new hacker's dictionary aux éditions mit press. certaines modifications apportées par eric s. raymond sont l'objet de controverses.

039 botnet

un botnet, contraction des mots robot et network, est une collection d'ordinateurs, en moyenne 20'000 mais pouvant aller jusqu'à plusieurs centaines de milliers, dont l'intégralité a été compromise et dont l'activité ou le contenu est contrôlé à distance par un hacker [005] ou un groupe de hackers [005]. on appelle ces ordinateurs des ordinateurs zombies. on estime qu'un quart des ordinateurs connectés à internet sont des zombies.
un botnet peut être utilisé pour de multiples raisons à commencer par le vol de données sensibles telles que numéros de séries des applications installées, noms d'utilisateurs, mots de passe et informations financières comme des numéros de cartes crédit, mais l'utilisation principale d'un botnet est de récolter des adresses email sur internet et d'envoyer des spams [008] depuis ses ordinateurs zombies.
un botnet sert aussi à perpétrer des attaques ddos [021] de façon massive en utilisant simultanément tous ses ordinateurs zombies comme cela s'est produit lors de l'attaque dont ont été victimes dans un premier temps les serveurs gouvernementaux estoniens, suivis par ceux des banques, des entreprises et des médias locaux fin avril début mai 2007. plusieurs dizaines de milliers d'ordinateurs zombies disséminés dans plus de 50 pays ont été utilisés ce qui rend la traçabilité de l'attaque extrêmement difficile. rien n'a été prouvé, mais le gouvernement russe et le russian business network [022] pourraient être à l'origine de cette attaque.

040 script kiddie

le script kiddie n'a peu ou pas de connaissances du code. il applique des logiciels créés par d'autres et des tutoriaux à la manière d'un livre de cuisine afin d'attaquer des systèmes, de s'introduire illégalement dans des ordinateurs ou de faire du vandalisme internet.
de fait, il s'agit généralement d'adolescents n'ayant pas les aptitudes pour être de vrais hackers [005] mais qui se servent des nombreux

outils à disposition pour impressionner leurs amis ou être reconnu dans les communautés de crackers [024].
un exemple typique est un adolescent de 15 ans dont le pseudo était mafiaboy. il s'est fait arrêté en 2000 dans une banlieue chic de montréal après avoir attaqué des site comme yahoo, dell, ebay et cnn et causé pour 7.5 millions de dollars de dommages au moyen d'outils téléchargés sur internet.

041 ascii art

l'ascii art est une pratique, proche du hacking [044] qui consiste à représenter une image à l'aide uniquement des 95 caractères imprimables sur les 128 que compte la charte ascii, american standard code for information interchange, crée en 1963.
la première trace de ascii art remonte à studies in perception 1, une pièce de kenneth knowlton, pionnier de l'art informatique, datant de 1966. cette pratique s'est popularisée vers la fin des années 70, début des années 80, du fait des limitations graphiques des ordinateurs personnels et des imprimantes.
une pièce importante du ascii art est deep ascii par l'ascii art ensemble en 1998. il s'agit d'une version de deep throat, film pornographique de 1972, transcodé en ascii et montré sur une machine du jeux d'arcade pong datant de la même année.
le ascii art peut être créer à la main dans éditeur de texte ou à l'aide de logiciels spécialement conçus pour transformer une image en texte. un emploi populaire de l'ascii art est l'utilisations des smileys ou émoticons tel le fameux sourire :-) ou encore l'étonnement o_0.

042 1984 network liberty alliance

le 1984 network liberty alliance est un groupe de programmeurs, d'artistes, d'activistes sociaux et de militants radicaux. le groupe se sert d'outils informatiques et des réseaux de télécommunication pour l'amélioration des conditions sociales, il est donc actif au sein du mouvement hacktivism [055].
le 1984 network liberty alliance a été créé en novembre 1984 lors d'un workshop des european peace marches en alsace. le nom vient du roman de georges orwell, 1984, et du rebel alliance de star wars.
ses membres fondateurs sont andré gorz, philosophe français, dov lerner, informaticien diplômé du mit, massachusetts institute of technology, gregoire seither, activiste de radio libre, frauke hahn, activiste

à la tête du greenham common women's peace camp, david szwarc du israeli peace movement et adama drasiweni, informaticien diplômé de l'université de londres et fondateur de n'da, premier réseau de télécommunication indépendant africain.
les autres membres importants de ce groupe sont mathew arnison, cofondateur de indymedia, peter makema, militant anti-apartheid sud-africain et uri avnery, activiste israélien pour la paix.
les activités du 1984 liberty network liberty alliance sont diverses. en 1985, celui-ci a prêté main forte à richard stallman, créateur du projet gnu [011], pour son free software mouvement. le groupe a aussi créé de nombreux bulletin board systems, serveurs accessibles par modem permettant l'échange de fichiers ou d'informations, au point d'avoir été accusé par le gouvernement allemand d'être un point de rencontre pour les activistes écologistes radicaux et les anarchistes en tout genre. depuis le g8 de 1998, le 1984 network liberty alliance fournit des centres de media alternatifs aux contre-manifestations lors de sommet de ce type.

043 spyware

un spyware, mouchard en français, est un malware [006] qui s'installe dans un système informatique à l'insu de son possesseur, de son utilisateur ou de son administrateur. le spyware est programmé pour collecter des informations de l'utilisateur sans que celui-ci s'en aperçoive.
après diffusion par internet ou au travers de freewares, logiciels gratuits, le spyware s'auto-installe à la manière d'un virus [054]. il procède ensuite à la collecte d'informations allant des habitudes de surf internet à des informations personnelles plus sensibles. finalement, le spyware envoie les données collectées à son programmateur au moyen d'internet.
si le spyware est généralement utilisé à des fins publicitaires, ainsi appelé adware, on peut lui prêter toutes sortes d'usages et on pourrait imaginer nombre de services de renseignements intéressés par un tel outil. à noter, qu'un spyware n'est généralement pas seul et est souvent accompagné de diverses autres infections informatiques.

044 hacking

le hacking est la pratique qui consiste à créer un hack [001], qu'il soit de nature matérielle ou informatique. au regret du hacker [005] original, l'expression est désormais communément utilisée pour par-

ler de piraterie informatique sur internet.
phreaking [029], phishing [035] ou ripping [002] sont différentes formes de hacking. les techniques de hacking les plus communes sont entre autres l'ingénierie sociale [015], le spoofing attack [012], le denial-of-service attack [021], le website defacement [009] ou le spamming [008]. les principaux outils utilisés sont le security exploit [023], le vulnerability scanner [053], le packet sniffer [019], le rootkit [036], le cheval de troie [046], le virus [054], le ver [031], le spyware [043], le malware [006] et le botnet [039].
la pratique du hacking a aussi mené au développement d'un dictionnaire informatique, le jargon file [038], d'une forme d'art visuel, l'ascii art [041], d'un argot informatique appelé leet ou leetspeaking [050], d'une éthique, hacker ethic [034] et d'un manifeste, hacker manifesto [013].

045 masters of deception

masters of deception, mod, est un des plus importants groupes de hackers [005] / phreakers [029] actif au début des années 90 et basé à new york. le nom est un pied de nez à leurs rivaux, le legion of doom, lod, [007], m étant un lettre au dessus de l. un tel acronyme leur permet aussi de se reconnaître tout en restant anonyme en situation sensible.
acid phreak, scorpion et hac ont fondé les masters of deception en 1989. ils ont été rejoints, entre autres, par mark abene « phiber optik » après que celui-ci ait quitté le legion of doom [007] en 1990.
les membres originaux des mod sont mark abene « phiber optik », paul stira « scorpion », eli ladopoulos « acid phreak », hac, john lee « corrupt » ou « netw1z » et julio fernandez « outlaw ». le groupe inclut 11 autres membres dont on ne connaît que les pseudonymes.
contrairement à la majorité de leurs semblables, les masters of deception ne partagent leur savoir avec d'autres hackers [005] hors mod uniquement si ceux-ci passent avec succès une sorte d'initiation à travers laquelle ils font preuve de respect et de responsabilité.
les masters of deception se sont opposé à leur groupe rival, le legion of doom [007], lors du great hacker war, la grande guerre des hackers qui s'est déroulée entre 1990 et 1991. bien que le legion of doom [007] prétende le contraire, les masters of deception seraient sortis vainqueurs de cette guerre grâce à leurs meilleures aptitudes. néanmoins, moins d'un an après, cinq membres des mod dont mark abene sont arrêté par le fbi.

046 cheval de troie – trojan

un cheval de troie, trojan en anglais, est un logiciel qui semble exécuter une certaine action, mais qui en réalité en exécute une autre. le principe est le même que le mythe de la grèce antique dont il tire son nom : il permet à un hacker [005] de s'introduire de façon dissimulée au moyen d'un leurre dans un système informatique.
si un cheval de troie n'est pas nécessairement malveillant, c'est souvent le cas. ce type de logiciel est devenu très populaire pour installer un backdoor, porte dissimulée permettant à l'attaquant de se reconnecter à tout moment avec le système infecté.
les six applications principales de trojans sont : l'accès à distance, la destruction de données, le téléchargement de données, l'utilisation de fonction de serveur, la déconnexion des logiciels de sécurité et l'exécution de denial of service attack [021].

047 logiciel open source

un logiciel open source est un logiciel dont la licence respecte les critères de l'open source definition établie par l'open source initiative, organisation créée en 1998 par bruce perens et eric s. raymond, détenteur du jargon file [038].
les dix critères de la licence open source sont les suivants : free redistribution, le logiciel peut être librement donné ou vendu ; source code, le code source doit être inclus ou disponible gratuitement ; derived works, les modifications et les travaux dérivés doivent être autorisés ; integrity of the author's source code, les modifications doivent redistribuées sous forme de patchs ou sous un autre nom ou numéro de version ; no discrimination against persons or groups, aucune discrimination envers une personne ou un groupe n'est tolérée ; no disrimination against fields of endeavor, aucune discrimination envers un domaine d'utilisation n'est tolérée ; distribution of license, les droits liés au logiciel doivent s'appliquer à tous ceux à qui il est redistribué ; license must not be specific to a product, les droits liés au logiciel ne doivent pas dépendre du fait que le logiciel fasse partie d'une distribution particulière ; license must not restrict other software, la licence ne doit imposer aucune restriction à un logiciel qui serait distribué avec le logiciel sous licence ; license must be technology-neutral, la licence ne doit pas imposer une technologie ou un type d'interface unique.

048 grey hat

le grey hat est un hacker [005] hybride. entre le black hat [033] et le white hat [018], il travaille à la frontière de la légalité. si on ne lui connaît pas toujours d'intentions criminelles, il ne se gêne pas pour outrepasser les lois pour arriver à des fins qui ne sont pas forcément évidentes.
il se différencie par le fait qu'il ne recherche jamais le profit personnel et, de même que le black hat [033], si ses motivations sont politiques, il est alors hacktivist [014].
on trouve aussi dans la catégorie du grey hat le hacker [005] qui s'introduit de façon illégale sur un serveur, mais qui ne fait qu'y laisser son nom sans rien voler ou modifier.

049 jed – jam echelon day

le 21 octobre 1999 s'est tenu le jed, jam echelon day. organisé par des hacktivists [014], ceux-ci ont tenté d'enrayer le système de surveillance echelon en le saturant de requêtes.
echelon est un système de surveillance mis en place dès les années 60 par les usa, le canada, la grande-bretagne, l'australie et la nouvelle zélande capable d'intercepter et d'analyser toutes les communications qu'elles soient émises par téléphone, fax ou email. le projet echelon a été maintenu secret jusqu'en 1988 lorsqu'un journaliste écossais le dévoile pour la première fois dans un article intitulé somebody's listening. le projet sera ensuite l'objet d'une enquête commanditée par le parlement européen.
sachant que le système réagit à certains mots-clé, des hacktivists [014] décident de le compromettre en le submergeant de requêtes. le 21 octobre 1999 a été déclaré jour de saturation du système echelon. les hacktivists [014] ont invité les internautes à se joindre à eux et à ajouter ce jour-là une liste de mots prédéfinis à leurs emails. personne n'a jamais su si cela avait fonctionné.
un second jam echelon day, jedii, s'est tenu en octobre 2000, mais sans rencontrer l'engouement de la première journée.

050 leet

le leet ou leet speak est une langue écrite codée propre à certaines communautés internet utilisant différentes combinaisons des caractères de la charte ascii, american standard code for information interchange, ressemblant aux caractères de l'alphabet latin pour remplacer ceux-ci.

l'origine du leet remonte au bulletin board system, serveurs accessibles par modem permettant l'échange de fichiers ou d'informations, durant les années 80. les initiés avaient le statut d'élite, elite en anglais, ce qui leurs donnaient accès à de nombreux fichiers auxquels le n00b ou newbie, néophyte informatique, ne pouvaient prétendre.
une autre théorie serait que le leet aurait été inventé sur les bulletin board systems pour contourner les filtres de textes empêchant les discussions sur des sujets interdits tel que le hacking [044].
le leet, autrefois réservé au hacker [005], cracker [024] ou autre script kiddie [040], s'est démocratisé et est désormais couramment utilisé dans les forums ou dans les communautés de joueurs de jeux vidéos.
le leet peut être codé de différentes manières, la plus simple étant juste de changer certaines lettres par des chiffres. par contre on peut le complexifier en utilisant tiret, barre oblique et symboles. cela permet d'avoir plusieurs niveaux de codage. ainsi leet speak peut s'écrire l33T 5p3ak, 1337 5p34k, £33‡ šp3@ķ ou encore |_ 33┬ _\┐°3/-\|<.

051 2600: the hacker quarterly

2600: the hacker quarterly est un magazine trimestriel américain qui traite aussi bien de différents sujets relatifs au hacking [044] que de news de l'underground informatique et libertaire. le magazine est publié par son fondateur, emmanuel goldstein, eric gordon corley de son vrai nom, et par 2600 enterprises, sa société à but non-lucratif.
le 2600 du nom du magazine correspond à la première fréquence en herz utilisée par les phreakers [029] pour hacker [044] les systèmes téléphoniques. quant au pseudonyme d'eric gordon corley, emmanuel goldstein, il s'agit de l'opposant à big brother dans 1984, le roman de georges orwell.
le magazine se définit par une pratique grey hat [048] du hacking [044], de sorte à garder une certaine neutralité entre white hat [018] et black hat [033].
2600 est non seulement à l'origine de h.o.p.e., hackers on planet earth, un hacker con [030] ayant lieu désormais tous les deux ans dans l'hôtel pennsylvania à new york, mais aussi de rencontres le premier vendredi de chaque mois à cinq heures, heure locale, dans une vingtaine de pays.
en 2001, le magazine a produit un documentaire sur kevin mitnick, le hacker [005] spécialisé en ingénierie sociale [015], traitant entre autre de son arrestation et du free kevin movement qui a suivi.

tsutomu shimomura, le hacker [005] ayant aidé le fbi à l'arrêter, avait précédemment proposé une autre version des faits dans takedown, son livre et son film du même nom. cette version fait l'objet d'une controverse.

052 cypherpunk

le cypherpunk s'intéresse à la protection des données privées, à la cryptographie et au crypto-anarchisme [020]. celui-ci communique à travers des mailing lists et met en avant des idées comme celle que chaque individu devrait protéger par lui-même ses données personnelles en utilisant des méthodes actives de cryptographie.
le terme, adjonction des mots cipher et punk, a été créé par jude milhon, hacker [005] et membre fondatrice du mouvement cypherpunk, pour parler de cyberpunks se servant de la cryptographie.
le pic d'intensité de ces mailing lists date de 1997 où après avoir été hébergé par toad.com, serveur crée par john gilmore, un hacktivist [014] célèbre, qui figure au rang des 100 plus vieux noms de domaine, elles ont été relayées par différents serveurs. à ce moment il pouvait facilement y avoir 200 emails échangés par jour comportant des débats personnels, des discussions politiques ou des informations techniques.

053 vulnerability scanner

le vunerability scanner est un logiciel informatique qui permet de rechercher les failles d'une application, d'un ordinateur ou d'un réseau de télécommunication. celui-ci peut être utilisé de façon malveillante, c'est alors un malware [006], ou bienveillante.
l'action se déroule en plusieurs étapes. dans un premier temps, le vulnerability scanner va chercher les adresses ip actives, adresses attribuées à chaque ordinateur se connectant à un réseau, les ports ouverts, les systèmes d'exploitations installés et les applications en cours d'utilisation. à ce moment, le scanner peut soit faire un rapport, soit aller directement à l'étape suivante qui consiste à déterminer le niveau de patch des systèmes d'exploitation et des applications. une fois toutes ces informations récoltées, le vulnerability scanner va tenter d'exploiter les failles ainsi découvertes.
le vulnerability scanner peut être utilisé pour faire la reconnaissance d'un réseau entier de sorte à s'en procurer l'accès et le contrôle de façon illégale.

054 virus

un virus informatique est un malware [006] qui se duplique et infecte un système informatique sans l'autorisation de son possesseur, de son utilisateur ou de son administrateur. il s'insère dans un paquet de donnés informatiques ou dans un autre logiciel. celui-ci est appelé hôte et lui sert de transport lors de sa duplication soit via le web soit à travers un support physique, cd-rom, clé usb, etc.
son nom provient de la similitude avec le virus biologique, tous deux utilisant la faculté de reproduction de leurs hôtes pour se propager. un virus informatique est incapable de se propager sans hôte.
certains virus ne sont programmés que pour se dupliquer et afficher un texte, une image, une vidéo ou encore un message audio. en revanche, d'autres sont programmés pour s'attaquer à la machine infectée en effaçant des fichiers ou même en formatant le disque dur. un des virus les plus destructeurs a été tchernobyl. il a été déclenché tous les 26 avril, jour de l'explosion de la centrale nucléaire russe, de 1998 à 2000 et s'est très largement répandu. il détruisait toutes les données du système infecté et rendait parfois même le matériel informatique hors d'usage.

055 hacktivism

l'hacktivism, hacktivisme en français, est la contraction des mot hack [001] et activism. cette idéologie consiste à se servir d'outils informatiques de façon non violente mais pas forcément légale dans le but de promouvoir des idées politiques. l'hacktivism part de l'idée que peu de gens connaissent le code, mais que le code affecte beaucoup de gens.
les moyens utilisés sont entre autres le développement de logiciels, tel freenet [016], la parodie de site web, le sit-in virtuel, le sabotage virtuel, le vol d'information, mais aussi le website defacement [009] et le dos attack [021]. ces deux derniers outils sont sujets à controverse, certains hacktivists [014] estimant qu'ils sont des attaques contre la liberté d'expression.
comme pour l'activisme conventionnel, les opinions concernant les moyens mis en œuvre sont partagées. certains estiment que les cyber attaques malveillantes sont une forme d'actions directes acceptables, voire nécessaires, alors que d'autres pensent que la résistance doit être pacifique et non destructrice.
le premier événement de l'histoire de l'hacktivism est l'attaque perpétrée en 1989 par le ver [031] wank contre le département américain de l'énergie, le réseau de recherche en physique des particules

et la nasa. celui-ci, une fois introduit dans un système informatique, remplaçait la page de login par ce message : worms against nuclear killers – wank – your system has been officially wanked – you talk of times of peace for all, and then prepare for war.
les autres événements de grande envergure sont notamment le **jed, jam echelon day, [049]** en 1999 et le **project chanology [025]** mis en place par les anonymous en 2008.
à cela s'ajoutent des projets moins connus comme les modifications effectuées en 1998 sur des sites indonésiens par des **hackers [005]** portugais appelant à l'autonomie du timor oriental ou encore la déconnexion des pare-feux chinois pour permettre l'accès à un internet non censuré par bronc buster, qui deviendra plus tard membre d'**hacktivismo [010]**.

Volume One, Issue 7, Phile 3 of 10

=-=

The following was written shortly after my arrest...

\/\The Conscience of a Hacker/\/

by

+++The Mentor+++

Written on January 8, 1986

=-=

Another one got caught today, it's all over the papers. "Teenager Arrested in Computer Crime Scandal", "Hacker Arrested after Bank Tampering"...

Damn kids. They're all alike.

But did you, in your three-piece psychology and 1950's technobrain, ever take a look behind the eyes of the hacker? Did you ever wonder what made him tick, what forces shaped him, what may have molded him?

I am a hacker, enter my world...

Mine is a world that begins with school... I'm smarter than most of the other kids, this crap they teach us bores me...

Damn underachiever. They're all alike.

I'm in junior high or high school. I've listened to teachers explain for the fifteenth time how to reduce a fraction. I understand it. "No, Ms. Smith, I didn't show my work. I did it in my head..."

Damn kid. Probably copied it. They're all alike.

I made a discovery today. I found a computer. Wait a second, this is cool. It does what I want it to. If it makes a mistake, it's because I screwed it up. Not because it doesn't like me...

Or feels threatened by me...

Or thinks I'm a smart ass...

Or doesn't like teaching and shouldn't be here...

Damn kid. All he does is play games. They're all alike.

And then it happened... a door opened to a world... rushing through the phone line like heroin through an addict's veins, an electronic pulse is sent out, a refuge from the day-to-day incompetencies is sought... a board is found.

"This is it... this is where I belong..."

I know everyone here... even if I've never met them, never talked to them, may never hear from them again... I know you all...

Damn kid. Tying up the phone line again. They're all alike...

You bet your ass we're all alike... we've been spoon-fed baby food at school when we hungered for steak... the bits of meat that you did let slip through were pre-chewed and tasteless. We've been dominated by sadists, or ignored by the apathetic. The few that had something to teach found us willing pupils, but those few are like drops of water in the desert.

This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.

Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.

I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike.

+++The Mentor+++

ressources

http://hacks.mit.edu/
http://www.dourish.com/goodies/jargon.html
http://www.catb.org/jargon/
http://www.catb.org/~esr/
http://www.webcrunchers.com/
http://www.digibarn.com/collections/newsletters/homebrew/
http://www.linuxfoundation.org/
http://www.kernel.org/
http://www.linux.org/
http://linux.com/
http://www.gnu.org/
http://www.stallman.org/
http://opensource.org/
http://perens.com/
http://creativecommons.org/
http://www.lessig.org/
http://www.eff.org/
http://www.wikipedia.org/
http://www.wired.com/
http://www.pekkahimanen.org/
http://www.stevenlevy.com/index.php/other-books/hackers
http://www.2600.com/
http://www.phrack.org/issues.html?issue=7&id=3#article
http://www.phrack.org/
http://www.textfiles.com/magazines/LOD/
http://www.textfiles.com/hacking/modbook1.txt
http://www.textfiles.com/hacking/modbook2.txt
http://www.textfiles.com/hacking/modbook3.txt
http://www.textfiles.com/hacking/modbook4.txt
http://www.textfiles.com/hacking/modbook5.txt
http://www.textfiles.com/
http://www.ccc.de/?language=en
http://chaosradio.ccc.de/
http://media.ccc.de/
http://www.wau-holland-stiftung.de/
http://www.cultdeadcow.com/
http://www.hacktivismo.com/
http://4chanarchive.org/brchive/dspl_thread.php5?thread_id=51051816
http://partyvan.eu/
http://iran.whyweprotest.net/
http://www.toad.com/
http://www.cypher.net/cyphernomicon.txt
http://www.torproject.org/
http://freenetproject.org/
http://www.summercon.org/
http://www.cultdeadcow.com/news/h-con94.txt
http://www.thelasthope.org/
http://www.defcon.org/
http://events.ccc.de/
http://www.knowltonmosaics.com/
http://www.ljudmila.org/~vuk/ascii/deep.htm
http://www.ljudmila.org/~vuk/ascii/throat.htm
http://www1.zkm.de/~wvdc/ascii/java/

merci à
jen estil, laure croset, nicolas tavaglione,
liliane schneiter et hervé graumann

v0.7b
genève, mai 2008 - tristan audeoud