Comment devenir un hacker ? - 1/8

Le hacking vous intrigue. Vous aimeriez en comprendre un peu plus sur ce sujet. Que quelqu'un vous indique où commencer ? Qu'est ce qu'un OS ? Le MBR ? NFS ? Comment fonctionne un virus ? Comment un programme peut s'incruster à votre insu ? Cet article est le premier de plusieurs articles sur le sujet.

J'ai écrit cet article pour répondre indirectement à la demande sur ce sujet, l'article "Comment devenir un hacker" étant limite insultant, à la fois pour les vrais hackers mais surtout pour vous, les lecteurs profanes, qui n'avez pas le temps pour comprendre comment ça marche ou parce que vous vous sous estimez sur vos capacités de compréhension.

Dans l'écriture de prochains articles, mon cousin Camille participera (pour la partie réseau).

Il est fort possible que vous ne deveniez jamais hacker, mais je vous promets, je me suis donné l'objectif que :

- Vous en saurez plus sur l'informatique et certains termes ésotériques : ils seront clairs pour vous !
- Vous serez capable de comprendre comment un hacker commence sa "carrière"
- De donner la passion à quelques uns ou unes --- comme cette partie de la communauté des précurseurs qui font de l'informatique par passion, et pas parce que c'est bien payé ou parce que papa a dit que c'était "un vrai métier"

Je suis donné l'objectif de construire une à une les marches du premier étage, pour qu'avec ces fondations informatiques, cette culture essentielle, vous puissiez vous attaquer à des sources plus complexes que j'ai sélectionné pour vous ; Des vrais articles écrits par des vrais hackers qui méritent le respect.
Dans ce premier article, je vous donnerai quelques bases --- sans encore les explorer --- de culture informatique, mais surtout des bases sur l'ordinateur PC --- et je vous expliquerai "d'où je viens".
C'est un article qui démarre "tout en bas", la compréhension de cet article vous sera plus évidente, suite aux articles suivants !

Je mettrais parfois trois étoiles derrière un terme --- ce terme sera expliqué en détails dans un article prochain.

Le second article sera consacré à l'utilisation d'un outil simple de lecture hexadécimal avec des exercices, nous reverrons ainsi des concepts évoqués dans le premier article : La pratique croisée à la connaissance théorique, le seul moyen de comprendre réellement !
Le troisième article, j'attaquerai l'assembleur et le langage machine, j'y mettrais beaucoup de fondations ---

Qu'est-ce qu'un hacker ?

Je ne me considère pas comme un hacker. Mais qu'est-ce qu'un **hacker** ?
Un hacker, étymologiquement est une personne qui "to hack", c'est-à-dire qu'elle "casse, qu'elle cisaille". Cette définition s'est ensuite un peu élargie à tout type de bidouilleur informatique. Maintenant, ça définit plusieurs types de profils de bidouilleurs informatiques, et la communauté des hackeurs vrais, excédée par son appropriation par des gogos ou des personnes mal intentionnées, a créé des termes plus spécifiques : Par exemple, lamer (un faux hacker), script kiddie (un mauvais codeur), cracker (casseur de programmes), etc...

Si vous avez vu Indiana Jones, vous avez une petite idée de l'esprit psychologique du hackeur : Un explorateur qui est capable d'enseigner à l'Université pour transmettre sa passion, mais qui préfère le terrain et les découvertes.

Comment devenir un hacker ? - 2/8

Beaucoup de ces nouveaux termes ont une connotation péjorative, alors que le hacker, traditionnellement, dans la communauté underground, a une connotation tout à fait positive.
Certains se retrouvent dans des séminaires (appelés party) où ils peuvent échanger des informations entre membres aguerris de cette communauté.

Vous vous doutez bien que le mérite d'un lamer qui modifie le code vbs d'un virus --- ne doit pas être le même qu'une personne qui prend le risque d'expliquer les failles d'un système ou d'une carte bleue (qui, hélas, a pour remerciement de la communauté étatique, qui n'y comprend rien --- une peine de prison !)

Dans mon esprit, le hackeur, c'est un artiste, un artiste de l'informatique, rarement connu, car invisible, qui fait de la compréhension des systèmes d'exploitations ou de réseaux, sa passion --- parfois rémunératrice. Ce n'est pas un anarchiste, même si dans son idéal de liberté, il aimerait que "les personnes en sachent plus", voire "que tout le monde soit libre" ---

Les hackers de très haut niveau sont très rares, peut être 200 dans le monde --- tournent autour d'eux, probablement 1000 à 2000 personne qui ont cet esprit là, et qui font des conférences pour échanger l'intelligence ainsi développée ---

Ils ne détruisent pas les données, n'écrivent pas de virus "pour se faire remarquer" ou "pour polluer les systèmes", effectuent peu de situations illégales (qui peuvent mettre en danger la vie d'autrui ou qui a des buts vénaux) ; Ils peuvent rentrer sur votre ordinateur sans que vous le sachiez et vous ne le sauriez jamais. Juste par curiosité ou challenge. Certains n'ont pas un profil "explorateur" mais plus "chevalier", ce sont eux qui travaillent à protéger des systèmes ou à écrire des antivirus.

A propos de l'anti article :
Je ne vous ferai pas l'affront de "apprendre l'anglais" ou "ne pas lire les RFC, ça sert à rien" ou faire "des mots croisés pour comprendre le cryptage".

Cet article est indigent pour plusieurs raisons :
- La première, c'est qu'il vous donne des connaissances erronées (comme l'ont mentionné plusieurs remarques, un exemple HTML n'est pas un langage de programmation --- mais de description !)
- La seconde, si ne vous connaissez pas l'informatique, vous ne comprendrez pas plus "le hacking", hélas !
- La troisième, le français...

Un article sur France Jeunes qui était plus proche du hacking, mais trop complexe pour les débutants, c'est **Introduction au Reverse Engineering**.

Je vous donne les connaissances sur les fondations (ça prendra quelques articles), et vous pourrez relire cet article, ensuite !

Ma légitimité sur le sujet

Nous devions être entre 1978 et 1981 environ. J'étais à la FNAC, dans le rayon informatique --- je vis une personne, il était en costume mais cool (ie. Sans cravate et avec un costume sympa, pas trop grisâtre) --- il y avait 3 personnes qui l'écoutaient devant un écran vert d'un Apple II --- Je lui dédie cet article --- Il apprenait comment désassembler les programmes --- à cette époque, cet écran vert qui affichait de l'hexadécimal (j'y reviendrai), c'était ... Magique !

Comment devenir un hacker ? - 3/8

Je n'ai pas osé l'approcher tellement j'étais intimidé, et en même temps fasciné !

C'est plus tard que j'ai décidé d'en faire mon métier, bien plus tard. J'avais un peu programmé, ça et là, sur différentes machines en Basic (un langage de programmation aisé à apprendre), plus pour comprendre les principes que pour développer une vraie application.

Un peu plus tard, une personne qui faisait un BEP électronique me dit de "m'acheter un PC" et "de me m'intéresser à l'assembleur". Je m'achetais donc un PC d'occasion (un Amstrad 1512 avec un disque dur de 20 Mo) auprès d'un ingénieur aéronautique qui m'aidait dans mes premières catastrophes (rires).

En Bts, je n'étais pas toujours un élève sérieux --- C'est en seconde année que j'ai eu envie d'apprendre l'assembleur tout seul (au lieu de réviser...) --- car je me rendais compte que le Cobol, c'était pas trop pour moi (en 1989-1990, de ma culture biaisée micro informatique, je trouve ça relou !).

De pctools à norton editor en passant par sourcer

J'avais déjà commencé à patcher (***) des jeux avec PCTOOLS (un utilitaire disparu à ce jour) ou éditer la FAT ou le MBR avec Norton Editor et m'intéresser un peu aux virus (j'avais eu plusieurs infections --- à ce moment, il existait peu d'outils, à part des scanneurs comme scan de macafee). Le système d'exploitation sur PC, c'était surtout MS/DOS (Microsoft) ou PC/DOS (IBM --- développé aussi par Microsoft).

Donc j'appris l'assembleur tout seul --- ou pour être plus exact avec un livre --- au départ, moi qui avait déjà un peu programmé en basic et en pascal, je trouvais ça tout à fait déroutant --- Je programmais parfois sans comprendre ce que je faisais --- puis comme nous échangions parfois quelques programmes, j'eus dans les mains, Sourcer (un désassembleur sous DOS) ; Avec avoir compilé quelques programmes avec MASM (***) et décompilé (***) tout à fait modestes, et en désassemblant avec Sourcer, ça fit --- les liens de compréhension : enfin !

Je me mis ensuite à m'attaquer au virus Cascade (alias 1701 ou 1704 --- longueur en octet du virus) qui m'intriguait car il était crypté puis je m'achetais une carte Thunderbyte pour être sûr de que ce je faisais --- découvrit le virus 896 (transmis à MacAfée à l'époque).

Donc pour résumer, ma légitimité sur cet article tiens sur :
- L'apprentissage de l'assembleur en autodidacte
- L'apprentissage des virus informatiques, seul, puis ensuite avec des sources de fanzines écrits par des hackers dignes de ce nom
- Mes premiers cours réseaux "micro informatique" à des ingénieurs réseaux aguerris en SNA ou X-25 (j'ai été administrateur Netware 3.12 en Token Ring)

Quelques repères historiques de l'informatique

Comme vous l'avez lu dans un précédent article, je vous ai indiqué que la micro-informatique est née en 1973. L'informatique, quant à elle, est née plus tôt, pour faire court, durant la seconde guerre mondiale --- les besoins de calcul pour guider les missiles, ainsi que les travaux de chercheurs en cybernétique et logique, comme Alan Turing ont permis la création du premier ordinateur : Le Zuse Z3 en 1941, le Mark I en 1944, le très célèbre ENIAC en 1946.

Comment devenir un hacker ? - 4/8

A cette époque là, il n'existait pas de langage dits de haut niveau (j'expliquerai ceci dans un prochain article), les informaticiens programmaient en langage machine.

Puis vint les premiers langages (dits de second niveau), les assembleurs.

Le développement des premiers langages de haut niveau, dits troisième niveau, s'est effectué entre les années 50 et 80 comme le Fortran (1956), Cobol (1959), le Basic (1963), le C (C++ en 1983 par Bjarne Stroustrup) ou le Pascal (1970).

En parallèle de ces développements de langages de programmation, les systèmes d'exploitations évoluèrent, et vint plusieurs types de systèmes dont les UNIX (dérivé du premier UNICS en 1969).

Les premiers hackers viennent probablement de ces années 1970 --- ce que je sais, c'est qu'une partie de l'esprit hacking est arrivé sur plusieurs technologies-faits-événements :
- L'utilisation de ressources réseaux initialement coûteuses téléphoniquement
- La protection de nombreux logiciels vendus par les éditeurs
- Les virus et les attaques par des chevaux de troie et les développements des BBS (une façon de partager des données) entre groupes de pirates
- Des systèmes d'exploitations parfois mal documentés par les éditeurs

Tous ces faits, ainsi que d'autres, ont contribué à un développement d'une compréhension plus active, certains informaticiens ou utilisateurs informatiques aguerris (power user) ont voulu creuser dans les profondeurs de ces systèmes.

Du binaire à l'hexadécimal

Je lis souvent que le code binaire est le code informatique : C'est partiellement erroné. Le code binaire est plus proche de l'électronique que de l'informatique !
Même si beaucoup d'informaticiens ont eu des cours sur le binaire, ce qui est le plus caractéristique, c'est l'hexadécimal !

L'hexadécimal, c'est un code dérivé du binaire, qui permet de coder sur 16 positions : de 0 à F, soit 0,1, 2 ... 9, A, B, C, D, E, F
Le code hexadécimal est souvent associé en 2 blocs, par exemple FF ou 0B ou 52.

L'hexadécimal est le code le plus important pour le hacker --- apprendre à le lire, et je vous expliquerai comment le lire --- pas tout de suite --- J'y reviendrais dans le second article. Il faut bien que je vous frustre un peu (la patience est la mère des vertus) ou vous mette l'eau à la bouche ;-)

De fait, beaucoup d'informaticiens qui travaillent dans le développement, travaillent sur des langages de "haut niveau", par exemple le C++ ou le PHP et peu développent en binaires ou lisent l'hexadécimal (sauf si vous êtes programmeur de jeux, de composantes électroniques ou ingénieur système sur MVS !)

Le système d'exploitation

Un système d'exploitation est un "logiciel spécial" qui vous permet d'utiliser votre ordinateur *facilement* . J'utiliserai souvent le terme OS, qui est l'équivalent anglais Operating System au lieu de Système

Comment devenir un hacker ? - 5/8

d'exploitation (trop long).

Il existe de nombreux OS sur le marché, je vous cite les plus connus ou répandus :
Sur les très grands systèmes informatiques (les ordinateurs peuvent occuper de très grandes salles), ils s'appellent z/OS (anc : MVS) ou VM, DOS/VSE sur IBM ou GCOS/7 sur Bull. Il existe des systèmes "moyens" (de la taille d'un très gros congélateur assez haut) qui utilisent le système d'exploitation VMS (anciennement sur Digital Equipment Corporation (Si je me souviens bien Bill Gates a fait ses premières expériences sur un DEC PDP/7 --- à vérifier), maintenant le constructeur Hewlett Packard) ou OS/400 (sur IBM)

Il existe plusieurs systèmes UNIX (un fonctionnant sur différentes types de machines (par exemple, les supercalculateurs Cray) ou sur des PC (Linux, BSD).

Sur PC, initialement, les OS étaient en mode texte (MS/DOS et PC/DOS, puis DR/DOS) avec une possibilité de faire fonctionner au-dessus une interface graphique (comme Windows ou GEM sur MS/DOS).
Ensuite est née, à partir de WINDOWS/NT (après la sortie de Windows 3.0), les systèmes d'exploitations en mode graphique. OS/2 était de ceux là.
Il existe donc "2 familles" de WINDOWS :
- Une qui se lance sur MS/DOS : Windows 1.0 à 3. X, Windows/95, Windows/98, Windows/Me
- Une qui est système d'exploitation graphique et est plus sophistiqué : Windows/NT, Windows/2000, Windows/Serveur, Windows/XP, Windows/Vista, Windows/Seven (***)

Il existe aussi des systèmes d'exploitations sur les téléphones portables, comme BlackberryOS, SymbianOS, Windows Mobile, IOS, etc...
Le système d'exploitation sur MAC est Mac OS, système propriétaire qui repose maintenant sur un noyau Unix depuis la version 10 (appelé aussi Mac OS X).

Revenons au vieux MS/DOS, un des premiers OS sur PC :
En MS/DOS, comme nous étions en mode texte (pas de souris, pas d'interface cool) le prompt (un signe du type c'est : \>) permettait de lancer un programme ou d'effectuer des commandes, par exemple (à chaque commande, un appui sur la touche entrée pour lancer la commande ---- d'où l'utilité du fichier à extension BAT (***) :
C : \> Format a :
(formate la disquette située dans le lecteur A)
C : \> Dbase
(lance le programme Dbase)
C : \> ver
(donne la version de MS/DOS (ou PC/DOS)

C : \> FDISK /STATUS
(donne une vision des partitions installées, MS/DOS ou autres)

Un PC "type"

Un PC est un micro-ordinateur basé sur "l'architecture x86" (***), il regroupe autour d'une Unité centrale (le gros boîtier), des périphériques d'entrées (c'est-à-dire du matériel qui permettent de "donner des données à l'ordinateur", par exemple le clavier, la souris ou le scanneur), des périphériques de sorties qui permettent "de sortir les données informatiques", par exemple l'écran ou l'imprimante.

Comment devenir un hacker ? - 6/8

Dans l'Unité centrale, nous avons plusieurs composantes :
Une carte mère : Elle est celle où va être incrustée différentes composantes électroniques comme le micro processeur, mais aussi une carte graphique, une composante qui gère votre clavier, plusieurs processeurs pour votre sortie USB, de la mémoire "RAM", etc...

Pour des raisons d'optimisation électronique (performance et fiabilité) cette carte mère s'est complexifiée et est un véritable plus réseau à part entière. Si le microprocesseur peut être considéré comme le cerveau de l'ordinateur, comme votre cerveau, celui-ci discute avec des organes --- Le microprocesseur ne travaille pas uniquement sur vos données, par exemple, lorsque j'utilise mon traitement de textes, il y a plusieurs activités informatiques "en fond", par exemple, parce que le système peut calculer autre chose, mettre des pages de mémoire pas utilisées depuis un certain temps sur le disque dur (ça s'appelle le swapping), etc.
Du point de vue électronique (et pas informatique), il y a des échanges de données, des "écoutes" sur des ports, etc...

Le fichier

IO. SYS, AUTOEXEC. BAT, COMMAND. COM, SOL. EXE, tous ceux-ci sont des fichiers.

Le fichier est la plus petite entité "logique" de l'ordinateur, un peu comme l'est la cellule d'un corps humain.
Les anciens fichiers sous MS/DOS comprenaient un nom de 1 à 8 caractères + une extension de 0 à 3 caractères (cette curiosité se destinait à faciliter le travail de portage de nombreux programmes fonctionnant sous CP/M un OS de Digital Research très bien implanté avant que n'arrive la déferlante du trio Microsoft-IBM-COMPAQ).

Sous WINDOWS, les extensions de fichiers ne se voient plus à travers l'interface, néanmoins, vous en rencontrez parfois à travers des incidents, par exemple, quand vous recevez un fichier à extension ODT, DOTX ou DAT que vos différents logiciels installés sur votre PC n'arrivent pas à lire (***).

Un fichier peut être de 2 types : Un fichier de données ou un fichier "programme" ; De fait, je n'entrerais pas dans les détails, mais il peut exister des variations de cette classification.

C'est grâce à l'extension du fichier, que nous pouvons savoir si c'est "un programme" ou "un fichier de données" ;
Un programme (je rappelle que ce que j'énonce est pertinent sur MS/DOS et "les WINDOWS") peut avoir une extension SYS, COM, EXE (***), etc...

Les extensions SYS étaient utilisées par Microsoft comme, à la fois, des fichiers programmes "de l'OS", mais aussi des fichiers de configuration de l'OS.

Notre premier exercice pour les neuneus

Sous WINDOWS, trouver la commande exécuter :
Puis tapez **cmd** (cmd exécute un programme qui va vous mettre en mode commande en ligne) ; Vous allez avoir une fenêtre de ce type

Comment devenir un hacker ? - 7/8

Remarquez que C:\Documents and Settings\Propriétaire.LUCIDE5678>
C'est le "prompt", ici, il indique que nous sommes dans le sous répertoire (dossier, c'est le terme windows) qui est Document and Settings, le \ indique un sous répertoire Propriétaire.Lucide5678.

Le petit trait qui clignote indique que vous pouvez entrer une commande.

Si vous entrez une commande inconnue, vous recevrez le message suivant (ex : j'ai tapé zorn) :
'zorn'est pas reconnu en tant que commande interne
ou externe, un programme exécutable ou un fichier de commandes.

Bon, maintenant, tapez **SET**
Il va nous envoyer un tas d'informations, chercher une ligne qui commence par PATHEXT.
Par exemple, sur ce poste, ma ligne est :
PATHEXT=. COM;. EXE;. BAT;. CMD;. VBS;. VBE;. JS;. JSE;. WSF;. WSH
Cette ligne donne tout les "extensions" qui sont des programmes exécutables sur cette version de WINDOWS.

Pour sortir de cette fenêtre, tapez **EXIT**

Exercices très simples :
- Quelle est la version de l'OS sur mon système ?
- Quelle est la version de votre OS ? (astuce : Il existe une commande (dans la partie démarrer, exécuter) qui permet d'afficher la boîte de dialogue indiquant la version --- je vous laisse chercher ---
- Quand vous tapez SOL (démarrer, exécuter), qu'est-ce qui se passe ?

Ce mode commande vous sera utile quelques fois, et vous permettra d'explorer certains arcanes du système. Ca vous permettra de plus facilement aussi de comprendre d'autres OS comme UNIX qui disposent aussi de commandes plus sophistiquées ou des outils qui ont été portés de l'UNIX vers WINDOWS.

Du réseau à tcp/ip

Comme vous le savez probablement, pour beaucoup d'entre vous, vous êtes connectés en réseau à travers un réseau qui s'appelle INTERNET.

Internet a été développé pour des besoins militaires (et oui, encore !) mais a vite envahi les Universités américaines en premier lieu et des autres continents.

Internet s'appuie sur une façon d'organiser l'échange des données entre ordinateurs : Ceci s'appelle un protocole.
Naturellement, quand vous rencontrez une personne dans nos contrées (le protocole peut être différent selon la culture), vous lui dites "bonjour" ou un informel "salut" "comment ça va", il en est de même pour tous les protocoles informatiques réseaux, c'est une façon à eux de communiquer pour échanger des données.

Il existe plusieurs protocoles réseaux dans l'informatique (bien moins nombreux que les OS), les plus répandus sont SNA (IBM), DSA (Bull).
Sur les systèmes micro informatiques, il a existé NETBEUI, IPX/SPX (Netware) ...

Sur les OS Unix et sur la plupart des WINDOWS à ce jour, le protocole est TCP/IP :

Comment devenir un hacker ? - 8/8

TCP/IP est l'acronyme de Transport Control Protocol et **Internet** Protocol

Le voilà notre **Internet** !

C'est grâce à ce protocole installé sur votre ordinateur que vous pouvez me lire --- Ou échanger des mails, partager des fichiers avec des logiciels comme emule, que vous pouvez aller visiter des sites grâce au web (qui n'est pas Internet mais une application, certes la majeure maintenant, du web --- celle-ci a été inventée au Cern par Tim Berners-Lee en 1989), etc...

Le succès du protocole TCP/IP, sa simplicité de mise en place (et sa diffusion sur de nombreux OS), la possibilité d'installer de nombreuses applications, puis l'explosion pour le grand public à travers le "WEB" a conduit à des sociétés informatiques spécialisées à développer des moteurs de recherche permettant de trouver des sites d'informations sur les domaines qui vous intéressent, de construire des outils de communication entre personnes d'ethnies différentes (bon, il faut partager le même langage tout de même) à travers des forums ou des "chat"), etc...

Tout ceci est TCP/IP !

Dans un cours ultérieur, je vous parlerai de TCP/IP plus en profondeur (ie. Technique).

Conclusion

J'espère que ça vous a plu et que ça été vivant (...) ; Le prochain article paraîtra dans 1 mois environ. Les réponses aux questions s'y trouveront.

Dans ce premier article, je vous ai donné :
- Un peu de culture informatique générale :
o Les systèmes d'exploitations
o Le fichier, entité "autonome"
o Le PC de façon simple
o L'hexadécimal
o Quelques briques sur les réseaux et TCP/IP

Pour compléter ces briques, même si ce n'est pas formellement utile au "hacking", je vous conseille quelques sites, à survoler ou lire de façon approfondie.

En anglais :
Sur la longue liste des systèmes d'exploitations : Les OS

En français :
Sur l'invention du WEB : Invention du Web
Sur la carte mère : Carte mère