Hacking éthique

Jason CHAMPAGNE
https://jasonchampagne.fr

Version : 3.0

Sommaire

Avant-propos

Ce court document au format PDF a pour but de présenter la **formation Hacking** que je propose sur ma chaîne YouTube.
Il va nous permettre d'aborder certains points essentiels des vidéos qui sont proposées : d'abord de vous présenter l'univers du hacker dans son ensemble, puis d'apporter un complément d'un point de vue juridique, pour mettre en garde contre les actes frauduleux et punis par les lois françaises, pour avoir une bonne pratique des techniques abordées dans le cadre de la sécurité informatique – ensuite, de détailler un peu plus les notions présentées au cours des séances qui sont ou seront publiées en ligne.

Merci de prendre le temps de lire ces notes et mises en garde, pour un hacking éthique, dans le respect des lois en vigueur.

Hacking, qu'est-ce que c'est ?

Le but de ce PDF n'est pas de vous dresser un historique complet du “phénomène” hacking, mais plutôt de vous apporter quelques précisions afin de mieux cerner l'environnement dans lequel vous vous apprêtez à arpenter les chemins.

Définition du hacker

Le terme “hacker” a pris tout son sens avec l'arrivée de l'électronique vers 1950. Il s'agit d'une personne curieuse d'esprit, qui se pose beaucoup de questions sur le fonctionnement d'un système ou d'un matériel.
En conséquence, ce dernier va bidouiller, détourner les innovations techniques en usant de ses hautes compétences en informatique (programmation, réseau, cryptographie, etc.) pour obtenir le résultat souhaité.

De là, je peux vous donner une définition simple et claire d'un hack : il est question de détourner le fonctionnement initial d'une chose (système, matériel, ...) pour lui faire produire un comportement non prévu à la base.
Par exemple, si vous parvenez à détourner votre voiture (censée se déplacer sur ses 4 roues, au sol) pour qu'elle puisse voler, on dira alors que vous avez hacké votre voiture.

D'une manière générale, on peut retrouver des hackers dans tous les domaines (même en agriculture), mais dans notre cas, nous nous intéressons plus précisément à l'informatique et tout ce qui en découle.

Acteurs dans le hacking

Dans le domaine, chaque hacker porte une “étiquette” qui détermine son type d'activité, sa démarche, ses opinions et ses objectifs sur le long terme.

D'abord, nous avons les “White Hats” qui traquent la moindre vulnérabilité et ne font rien d'illégal. Au contraire, ils avertissent les éditeurs des systèmes à risque pour les aider, voire leur proposer des correctifs.
À l'inverse nous avons les “Black Hats” qui eux cherchent directement le profit, la vente de données personnelles (ventes sur le marché noir)...ils font dans l'illégalité et dans un cas extrême, on les nomme “Hacktivists” (*comme les Anonymous*). Entre

ces opposés se trouve les “Grey Hats”, bien que ces derniers emploient aussi des méthodes illégales pour arriver à leurs fins mais se considérent comme neutres aux yeux de la Loi.

Il existe bien d'autres manières de qualifier les personnes faisant du hacking, mais avec ces quelques termes, vous devriez déjà y voir plus clair.

Méthodes employées autour du hacking

Volontairement, je ne vais vous parler que des méthodes les plus courantes en hack. Parmi elles, on y trouve des activités que la Loi n'interdit pas...et d'autres qui rentrent dans le cadre du délit ou du crime.

Recherche de failles et exploits	Chercher des failles et vulnérabilités dans des programmes afin de modifier le comportement attendu par ces derniers. Cela revient à chercher une erreur et inventer une technique pour s'en servir.
Intrusion	Accéder à un système informatique, l'utiliser, exécuter du code non autorisé sur un serveur appartenant à une entreprise, etc.
Défaçage	Modification des fichiers d'un site web, dans l'unique but de montrer au public la réussite du hack, ou proposer une toute autre page, diffuser un message.
Utilisation des données	Collecte, traitement et vente de l'information à autrui. L'auteur peut user de programmes malveillants pour espionner la victime et récolter des données privées.
Déni de service (DOS)	Bloquer le fonctionnement d'un système en le paralysant. Par exemple, en encombrant le serveur de requêtes multiples, celui-ci finit par crasher et entraîner des problèmes.
Espaces en ligne	On les nomme les dépôts (ou “repositories”), ce sont des sites web prévus pour contenir de la

	documentation, des outils et/ou exploits en tous genres.
Phreaking et espionnage	Détourner l'usage des systèmes téléphoniques, en vue d'intercepter des conversations, les écouter, ou de pouvoir passer des appels gratuitement et ne pas payer des services payants.
Virus, vers et trojans	Programmes qui infectent à votre insu un système, peuvent espionner et récolter des informations, corrompre des données, avoir un fonctionnement non autorisé.
Social Engineering	Manipuler une personne, gagner sa confiance ou profiter de sa naïveté pour lui soutirer des informations confidentielles, s'en servir de complice pour commettre un acte illégal.

Et puisqu'il y est question de lois, je vous invite dès maintenant à consulter la suite du PDF, pour entrer un peu plus dans le vif du sujet.

Hacking, ce que dit la Loi française

Je vais vous présenter les quelques articles relatifs au hacking, avant d'apporter quelques commentaires sur ce qui est légal ou punissable.

Code pénal - article 323-1

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.

Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende.

Code pénal - article 323-2

Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 150 000 € d'amende.

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende.

Code pénal - article 323-3

Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende.

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende.

Code pénal - article 323-3-1

Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Code pénal - article 323-4

La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Code pénal - article 323-5

Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :

1. L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26 ;
2. L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;
3. La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;
4. La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;
5. L'exclusion, pour une durée de cinq ans au plus, des marchés publics ;
6. L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré

ou ceux qui sont certifiés ;

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

Code pénal - article 323-6

Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre encourent, outre l'amende suivant les modalités prévues par l'article 131-38, les peines prévues par l'article 131-39.

L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

Code pénal - article 323-7

La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines.

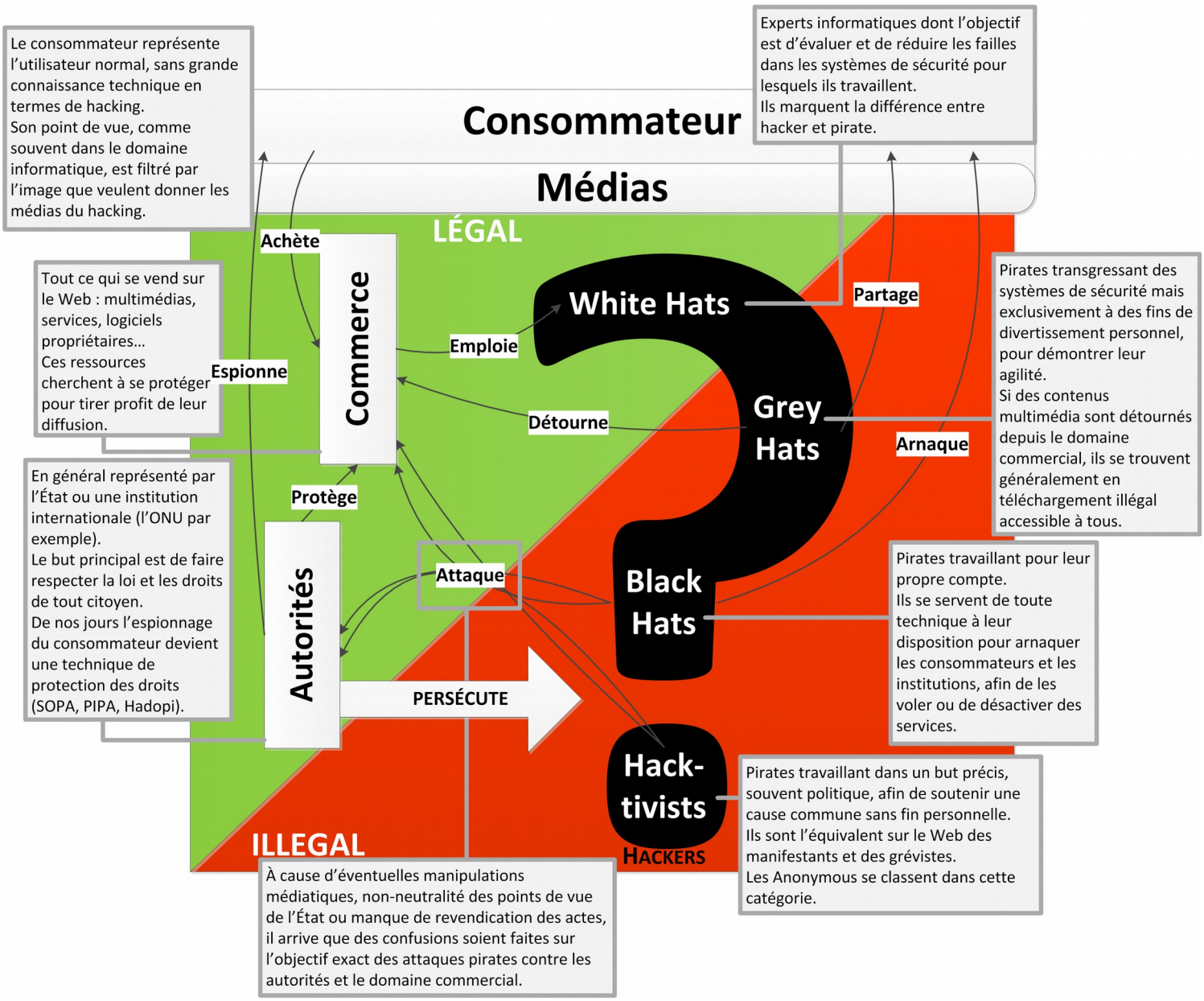
Réponses aux questions les plus courantes

Retrouvez à présent quelques réponses à des questions “bêtes” ou récurrentes que beaucoup se posent lorsqu'ils s'intéressent à la sécurité informatique.
Bien évidemment, on pourrait en faire des livres complets, mais j'ai tenté de sélectionner ce qui me semblait le plus parlant, et de donner mon propre point de vue sur ces quelques interrogations.

<u>Un hacker est-il un pirate ?</u>

- À la base, un hacker représentait toute personne capable de prouesses en informatique pour trouver des failles dans les systèmes, savoir analyser des architectures, et user de toutes les technologies et langages disponibles pour les exploiter, contourner des sécurités, adapter un programme. Malheureusement, les médias et/ou gouvernements ont très vite associé le terme de “hacker” uniquement aux personnes malhonnêtes, celles qui volent les données des utilisateurs, font de l'espionnage industriel, détournent de l'argent...ou pire.
  Tout n'est donc qu'une question d'actes et de point de vue. Le hacker qui vole des données bancaires pour s'enrichir est un “mauvais” hacker (ou pirate) – le

hacker qui détecte des failles de sécurité sur un programme comme Google Chrome et en avertit la société en privé pour l'aider à la correction des vulnérabilités est un bon hacker (voir les termes “White Hats” et “Black Hats” évoqués plus hauts).



Crédit : http://ethique-tic.fr

Est-il légal de faire du hacking ?

- Il va m'être difficile de faire court sur cette question, mais pour rester simple, il est parfaitement légal de se former à des techniques de programmation, à faire de la recherche et exploiter son matériel, tant que cela ne vient pas se confronter aux lois citées plus haut.
  Par ailleurs, il ne vous est pas interdit de hacker votre propre matériel (et non celui de vos parents) par simple curiosité, ou pour tester la sécurité de vos équipements.

L'idéal est donc de mettre en place un petit environnement de développement (via une machine virtuelle) et de mettre en application ce que vous allez apprendre sur vos propres systèmes et infrastructures, tant qu'ils vous appartiennent.
Pour le reste, vous devez disposer d'une autorisation écrite et explicite d'un tiers pour exploiter son système/infrastructure. À l'inverse, vous vous exposez à des peines !

Devenir hacker est-il difficile ?

- Sans vouloir jouer les philosophes, l'apprentissage de toute chose commence par un premier pas...et il n'y a pas de chemin plus facile qu'un autre...juste différentes manières d'arriver à destination.
  En d'autres termes, devin hacker est un travail de longue haleine, régulier mais captivant, à l'instar du pratiquant d'arts martiaux qui consacre sa vie pour son art, le vit au quotidien et ne cesse de se perfectionner.
  Alors de la difficulté, il y en aura, des cas qui semblent insurmontables...sans doute également, mais rien d'humainement impossible. Le temps, la patience, et la bonne application de vos compétences auront raison de tout. Et avec une dose suffisante de confiance en vous, vous deviendrez un très bon hacker.

Faut-il connaître l'anglais pour progresser ?

- C'est un fait, et depuis toujours. La majeure partie des systèmes, des langages de programmation, des logiciels et matériels informatiques ont été inventés et/ou confectionnés en grande partie par des Américains.
  En toute logique, chaque documentation originale, chaque architecture, chaque technologie est diffusée en anglais. Maintenant, il n'est pas nécessaire d'être bilingue pour vous en sortir...et il est toujours plus facile pour quelqu'un de retenir des termes étrangers dès lors qu'ils se rattachent à une passion.
  Enfin, l'anglais est omniprésent dans le monde, à chaque fois que vous regardez vos messages, consultez vos e-mails, allez au travail, prenez la voiture, cuisinez... Comme tout le monde, vous vous y ferez très bien !

Si vous avez d'autres questions, je vous invite à me les poser dans les commentaires des vidéos de la formation ou sur les réseaux sociaux.

Hacking, ce que nous allons apprendre

Avant tout, vous comprendrez qu'il est humainement impossible d'aborder toutes les spécificités de la sécurité informatique. D'ailleurs, il est possible que vous vous formiez à d'autres techniques, appreniez d'autres langages et il n'est donc pas possible de trouver via cette formation un listing exhaustif.

Pour autant, nous allons essayer d'aborder un maximum de points essentiels. En partant des bases et de ce qui se faisait historiquement pour ne pas négliger les menaces modernes qui font le quotidien des particuliers et des entreprises d'aujourd'hui.
N'oubliez pas que le hacking vit, évolue au gré de l'innovation et de nombreuses nouvelles méthodes, toujours plus sophistiquées les unes que les autres.

Programmation

La programmation est un passage obligatoire lorsque l'on fait du hacking. Il s'agit d'étudier et d'apprendre à utiliser divers langages en informatique (C, C++, Python, PHP, Shell, etc.) en vue de comprendre le fonctionnement des machines, des appareils électroniques, des systèmes et des réseaux.

Par ailleurs, acquérir des connaissances en programmation vous permettra de développer à votre tour des outils pour gagner du temps, automatiser des tâches, réaliser un audit de sécurité, exploiter une faille ou simplement pour améliorer un logiciel open source.

Rappelez-vous, un hacker est une personne capable de rendre “élégant” son code. Il ne s'agit pas simplement de faire fonctionner un programme, mais que ce dernier s'exécute de la meilleure manière qui soit !

Réseaux et télécomunnications

Les réseaux et télécommunications font transiter sans cesse de l'information. Que ce soit par Internet, le Web, les réseaux téléphoniques – ces différents moyens de communication présentent eux même leurs propres failles de sécurité.

Que faire si une communication est interceptée ? Comment éviter l'espionnage ? Peut-on encore échanger de l'information sans que celle-ci ne soit divulguée

publiquement ?
Nous répondrons à ces quelques questions quand nous étudierons l'aspect “réseau” de la sécurité en informatique. Ce sera également l'occasion de se pencher sur quelques normes internationales et se servir d'outils associés pour consolider vos compétences.

Systèmes d'exploitation

Les systèmes, vous les connaissez très bien, ce sont ceux que vous utiliser tous les jours sur vos ordinateurs (Windows, GNU/Linux, BSD, Mac OS), sur vos appareils mobiles (Android, iOS, BlackBerry, ...) ou que l'on retrouve sur les millions d'appareils partout dans le monde, sur tous les domaines (médical, aéronautique, automobile, etc.)

Comprendre son système, c'est prendre conscience de ses faiblesses, identifier rapidement ses vulnérabilités et savoir se prémunir des menaces.
Le hacking a donc sa place ici, dans l'objectif de sécuriser ces systèmes ou à l'inverse, user de méthodes ingénieuses pour rechercher des vulnérabilités et les tirer à son avantage, toujours dans la légalité.

Cryptologie

La cryptologie est une “science” qui fait appel à des notions mathématiques et des méthodes algorithmiques plus complexes pour englober certains aspects que sont la cryptographie, la cryptanalyse ou dans une moindre mesure la stéganographie.

Si ces termes vous font peur, ça n'est pas bien grave. Nous aurons grandement l'occasion d'étudier des manières de chiffrer de l'information, de la décoder ou la décrypter, d'analyser un programme protégé ou même de révéler les secrets cachés dans un fichier en apparence normal.

Le petit mot de la fin

Vous l'aurez compris après une lecture attentive, le hacking est un domaine très sérieux demandant une certaine maturité. Même si on l'associera volontiers à de la sécurité informatique, il convient de rappeler que tout n'est pas permis et que votre pratique doit se cantonner au respect des lois de votre pays (pour nous en majorité, il est question de la France, mais le piratage est puni où que vous soyez).

Je ne pourrai en aucun cas être tenu pour responsable de vos actes frauduleux et faits allant à l'encontre de la Loi.

En suivant mes formations, vous acceptez l'entièreté dudit document et vous engagez à utiliser les compétences acquises pour de bonnes pratiques ou sur un environnement de test qui vous appartient (type “environnement de laboratoire”).

Jason CHAMPAGNE

Annexes

Envie de plus de renseignements ou de vous former davantage avant de vous lancer ? Voici quelques liens qui devraient vous intéresser.

Pour une grande partie d'entre eux, l'utilisation des logiciels cités plus bas est détaillée dans certaines vidéos ou sur d'autres PDF proposés sur ma chaîne.

Quelques sources

- Lois françaises [https://www.legifrance.gouv.fr]
- Légitimité du hacking [http://ethique-tic.fr]
- Wiki Backtrack [http://wiki.backtrack-fr.net]

Quelques formations en vidéo

Retrouvez sur ma chaîne d'autres formations en vidéo qui vous seront sans doute utiles lors de votre progression dans le domaine du hacking :

- C
- GNU/Linux
- Python
- HTML 5 et CSS 3
- PHP et SQL

Quelques outils

Quelques éditeurs de code avec coloration syntaxique pour faire ressortir les mots-clés des langages de programmation, gagner en lisibilité et en confort :

- Atom [https://atom.io]

- Brackets [http://brackets.io]
- Notepad++ [https://notepad-plus-plus.org/fr/]
- Sublime Text [https://www.sublimetext.com]
- Visual Studio Code [https://code.visualstudio.com/]

Un support de développement pour Windows ou un compilateur et débogueur séparés pour plus de flexibilité :

- GCC [https://gcc.gnu.org]
- GDB [https://www.gnu.org/software/gdb/]
- MinGW [http://www.mingw.org]
- Valgrind [http://valgrind.org]

Un serveur HTTP tournant sous Apache ou Nginx, selon vos préférences, pour tout ce qui est axé sites internet et réseau :

- Nginx [http://nginx.org]
- XAMPP [https://www.apachefriends.org/fr/index.html]

Un client FTP pour déployer vos applications et les tester en ligne :

- FileZilla [https://filezilla-project.org]

Quelques outils complémentaires, comme un interpréteur de langage Python ou Git pour créer des dépôts de vos projets et gérer plusieurs versions :

- Git [https://git-scm.com]
- Python [https://www.python.org]

EOF