Le guide complet pour commencer la Cybersécurité en 2024.

par Hafnium.

1. A qui s'adresse ce guide ?

Ce guide s'adresse aux personnes qui veulent débuter dans la sécurité informatique mais qui ne savent pas par où commencer.

En effet, sur Internet, sur YouTube, et sur les différents réseaux sociaux, on trouve souvent des informations assez contradictoires, ce qui peut rendre difficile de filtrer ce qui est utile ou non.

Le but de ce guide est qu'après l'avoir lu, vous ayez une image beaucoup plus claire de ce qu'est le monde de la cybersécurité et des actions à mettre en place pour démarrer dans ce milieu.

Sur ce, je vous souhaite bonne lecture :)

2. Pourquoi la cybersécurité est-elle nécessaire ?

Contrairement à ce que l'on pourrait croire, il n'est pas si simple de trouver un emploi dans la cybersécurité.

Étant freelance, j'ai eu des difficultés à trouver des clients malgré mes compétences et mon expertise dans le domaine, surtout au début.

Le principal problème pour les entreprises est que la cybersécurité ne génère pas de revenus directs.

- Faire un audit de sécurité interne coûte de l'argent.
- Mettre en place des mesures de protection coûte de l'argent.
- Employer des experts en cybersécurité coûte de l'argent.

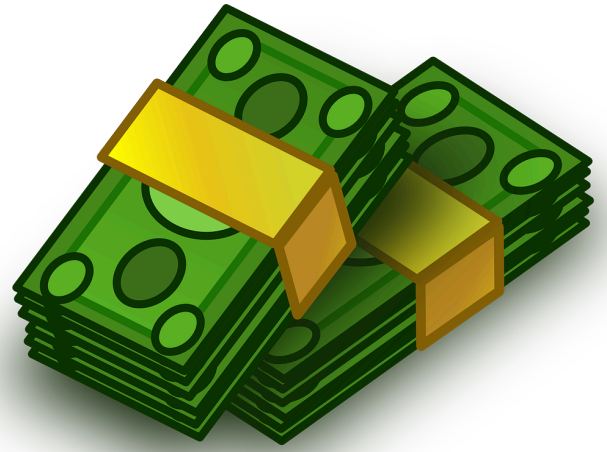
Malheureusement, toutes ces dépenses n'apportent pas de bénéfice tangible aux clients du produit final. Par exemple, contribuer à sécuriser la plateforme YouTube est important, mais il est souvent perçu comme économiquement plus viable à court terme d'ajouter de nouvelles fonctionnalités et d'employer des développeurs.

La cybersécurité est souvent vue comme quelque chose d'optionnel par les entreprises. Cela signifie que réaliser un audit de sécurité n'est pas une priorité pour la plupart, surtout pour celles qui ont moins de ressources.

Résultat : les entreprises “économisent” de l’argent à court terme, mais à long terme, lorsque survient une attaque, les coûts des dégâts sont en moyenne 10 à 100 fois supérieurs à ceux d’un audit.

Mais à ce moment-là, il est trop tard.

Une grande partie du travail consiste donc à convaincre les entreprises de l’utilité réelle de la cybersécurité, même si cela nous paraît évident.



3. Quels sont les types de hackers ?

Avant d’énumérer les types de hackers, répondons à la question : qu'est-ce qu'un hacker exactement ?

Un hacker est quelqu'un qui parvient à détourner un objet de son utilisation initiale pour lui faire accomplir ce qu'il veut.

Par exemple, la manipulation psychologique est une forme de “hacking d'êtres humains”. Le manipulateur fait faire à sa victime ce qu’il veut par tous les moyens possibles (biais cognitifs, mensonges, chantage, etc.).

Faire cuire un œuf sur le moteur d’une voiture est également possible, bien que ce ne soit pas l'utilisation initiale du moteur. Cela peut donc être vu comme du hacking (bien que ce soit inhabituel, des gens l'ont déjà fait pour s’amuser).

Le hacking informatique consiste à détourner un système informatique de son utilisation initiale pour lui faire faire ce que l'on veut. Cela peut être absolument n'importe quoi.

Par exemple, imaginons que vous installiez un site web sur votre serveur dont le but est d'afficher votre CV. Des hackers peuvent, s'ils le souhaitent, détourner votre serveur de son utilisation initiale pour :

- voler des informations confidentielles,
- mettre le système d'un concurrent hors service,
- lancer des attaques de ransomware depuis votre serveur,
- ou même faire tourner un serveur Minecraft sur votre mini-serveur (c'est simple, mais cela correspond à la définition du hacking).

En général, on distingue trois types de hackers :

3.1 Les Black Hats (Chapeaux noirs)

Les Black Hats font partie des "hackers malveillants". Leur but est de causer des dégâts ou de voler des informations confidentielles en exploitant une faille de sécurité et en détournant le système informatique de son utilisation initiale.

Petite parenthèse, vous avez peut-être déjà entendu le terme "script kiddie".

Beaucoup de Black Hats, qui ne sont pas compétents techniquement, sont appelés des "script kiddies".

Ce sont des individus avec de faibles compétences techniques qui utilisent des outils créés par d'autres personnes plus compétentes pour causer des dégâts (parfois même sans faire exprès).

Certains systèmes informatiques mal protégés sont vulnérables, ce qui suffit à causer des dommages.

3.2 Les White Hats (Chapeaux blancs)

Les méthodes des White Hats et des Black Hats sont similaires, mais leur objectif est différent. Le but des White Hats n'est pas de causer des dégâts ou de voler des informations confidentielles. Leur mission est de protéger le système d'information.

Évidemment, le White Hat doit avoir l'accord écrit de l'entreprise pour laquelle il travaille, sinon cela peut être considéré comme illégal (voire criminel dans certains pays). Leur rôle est de sécuriser le système afin que, si un Black Hat tente de l'exploiter, il soit incapable d'en tirer avantage.

3.3 Les Grey Hats (Chapeaux gris)

Les Grey Hats ressemblent aux Black Hats à bien des égards. La principale différence est qu'un Grey Hat agit sans l'accord explicite de l'entreprise ou de l'organisation.

Par exemple, certains Grey Hats s'introduisent illégalement dans un système informatique pour prévenir "gentiment" les propriétaires que le système est vulnérable.

D'autres le font juste pour s'amuser et se lancer des défis, trouvant parfois cela "rigolo" et "enrichissant".

La différence principale avec les Black Hats réside dans l'intention : le but des Grey Hats n'est PAS de causer des dégâts.

Notez que tous les professionnels sérieux en cybersécurité sont des White Hats, moi y compris.

4. Quels sont les métiers dans la cybersécurité ?

Le terme cybersécurité, ou sécurité informatique, est assez vague et englobe de nombreux aspects différents.

Il existe des dizaines de métiers dans ce domaine, mais je ne vais pas tous les lister ici. Voici cependant les cinq métiers les plus courants :

4.1 Analyste SOC

SOC signifie **Security Operations Center**. Un analyste SOC est employé par une entreprise pour :

- Analyser les menaces en temps réel

- Inspecter les logs (fichiers texte contenant des informations sur l'exécution des services) du pare-feu et des différents services
- Répondre aux incidents en temps réel
- Assurer la maintenance et les mises à jour des systèmes
- Analyser le trafic réseau pour détecter d'éventuelles menaces

Pour simplifier, imaginez qu'il y a un mur qui sépare le système informatique de l'entreprise et le monde extérieur.

L'analyste SOC est celui qui se trouve dans la tour de contrôle et veille à ce que personne ne franchisse ce mur. C'est souvent le premier métier dans la cybersécurité pour beaucoup de débutants.

4.2 Pentester

Le pentester peut être employé par une entreprise ou travailler en indépendant (freelance). Son rôle est de simuler une attaque sur un système informatique, c'est-à-dire reproduire ce qu'un "black hat" ferait, et de signaler tous les problèmes trouvés. Ensuite, il rédige un rapport détaillant :

- Les failles de sécurité
- Les problèmes de configuration
- Des recommandations pour corriger ces problèmes
- La gravité de chaque problème

On l'appelle aussi le "hacker éthique", car il "hacke" pour le bien de l'entreprise sans causer de dégâts.

En reprenant l'analogie du mur, **le pentester est celui qui liste toutes les manières de casser ou de contourner le mur pour s'infiltrer dans l'entreprise.**

C'est probablement le métier le plus connu en cybersécurité.

4.3 Analyste Forensique

Imaginez qu'un crime a eu lieu.

Deux jours plus tard, un suspect est arrêté.

Pour savoir si c'est le coupable, une des méthodes consiste à examiner les appareils numériques du suspect.

C’est le rôle de l’analyste forensique (digital). Il fouille le PC du suspect pour retracer son activité et collecter des preuves d’un éventuel crime.

Compte tenu de toutes les informations que nous laissons sur nos appareils, il est relativement simple de trouver des indices (fichiers, messages, artefacts Windows, etc.).

Les analystes forensiques sont bien équipés avec des outils avancés qui peuvent retracer presque en un clic ce que vous avez fait sur votre ordinateur.

4.4 Bug Bounty Hunter

Le bug bounty hunter est un métier un peu différent. Il ne travaille pas pour une entreprise en particulier, n’a pas de contrat de travail ni de mission spécifique (contrairement au pentester freelance, par exemple).

Comment cela fonctionne-t-il ?

Des entreprises comme Microsoft, OVH, Doctolib, etc., annoncent sur leur site : “Celui qui trouve des failles de sécurité dans notre infrastructure sera rémunéré.”

Évidemment, il y a des règles :

- La rémunération dépend de la gravité de la faille
- C’est le premier à trouver la faille qui touche la récompense
- Certaines parties du site/serveur sont exclues

Ainsi, au lieu d'embaucher un pentester, l'entreprise fait travailler des milliers de personnes "gratuitement" et ne paye que pour chaque faille découverte.

Il n'y a pas de barrière à l'entrée pour devenir bug bounty hunter, donc la concurrence est très rude, ce qui fait que dans la plupart des cas, il est plus rentable d'être employé en tant que pentester dans une entreprise classique.

Le site le plus connu est probablement https://hackerone.com, qui répertorie les programmes de bug bounty de milliers d'entreprises.

4.5 Cyber Police / Enquêteur OSINT

OSINT signifie Open-source Intelligence.

Imaginons que notre suspect de meurtre soit caché dans un autre pays et que nous n'ayons pas accès à ses appareils numériques.

Nous ne pouvons donc pas faire d'analyse forensique digitale.

Cependant, au lieu de fouiller ses appareils, nous pouvons tenter de collecter toutes les informations accessibles sur internet (d'où le terme open-source) pour essayer de trouver des preuves de son implication dans le crime (d'où le terme intelligence).

Les policiers ont des pouvoirs spéciaux, car ils peuvent demander aux hébergeurs de services sur le territoire national (serveurs, opérateurs, bases de données) de divulguer des informations supplémentaires sur le suspect (adresse IP, numéro de téléphone, géolocalisation) pour aider l'enquête.

5. Quelles sont les étapes d'un test d'intrusion ?

Dans cette partie, je vais vous parler des tests d'intrusion et de leur déroulement, car je suis moi-même pentester freelance 🙂

Tout d'abord, qu'est-ce qu'un test d'intrusion ?

Un test d'intrusion est réalisé par un pentester afin de simuler une attaque semblable à celle qu'un black hat pourrait mener. L'objectif est d'identifier les vulnérabilités potentielles dans le système informatique.

Il existe plusieurs types de tests d'intrusion :

1. **Tests en boîte noire (black box)** :
    - Vous n'avez aucune information préalable sur l'entreprise.
    - Vous êtes dans la position d'un attaquant externe (black hat), cherchant à découvrir et exploiter des vulnérabilités sans informations internes.
2. **Tests en boîte blanche (white box)** :
    - Vous disposez de toutes les informations nécessaires sur l'entreprise, y compris ses systèmes et infrastructures.
    - Vous devez identifier toutes les vulnérabilités potentielles avec une vue complète de l'environnement.
3. **Tests en boîte grise (grey box)** :
    - Vous avez accès à certaines informations internes, comme un compte utilisateur avec des privilèges modérés.
    - Vous combinez des éléments des deux approches précédentes.

Le choix de la méthode dépend de la taille de l'entreprise, du budget (les tests en boîte blanche étant souvent plus coûteux en raison du volume d'informations à traiter) et de la confiance accordée au testeur d'intrusion (pentester).

Une fois le contrat signé et le type de test sélectionné, le test d'intrusion peut commencer. Voici la méthodologie générale souvent utilisée :

5.1. Énumération

La première étape consiste à recueillir un maximum d'informations sur le système informatique du client :

- Quelles sont les machines et comment sont-elles organisées ?
- Quels services/logiciels sont utilisés ?
- Quels ports sont ouverts ?
- Quelles sont les fonctionnalités du produit ?

Le but est de comprendre au mieux la cible sans nécessairement chercher à trouver des failles de sécurité. L'OSINT (Open Source Intelligence) est également utilisé à cette étape.

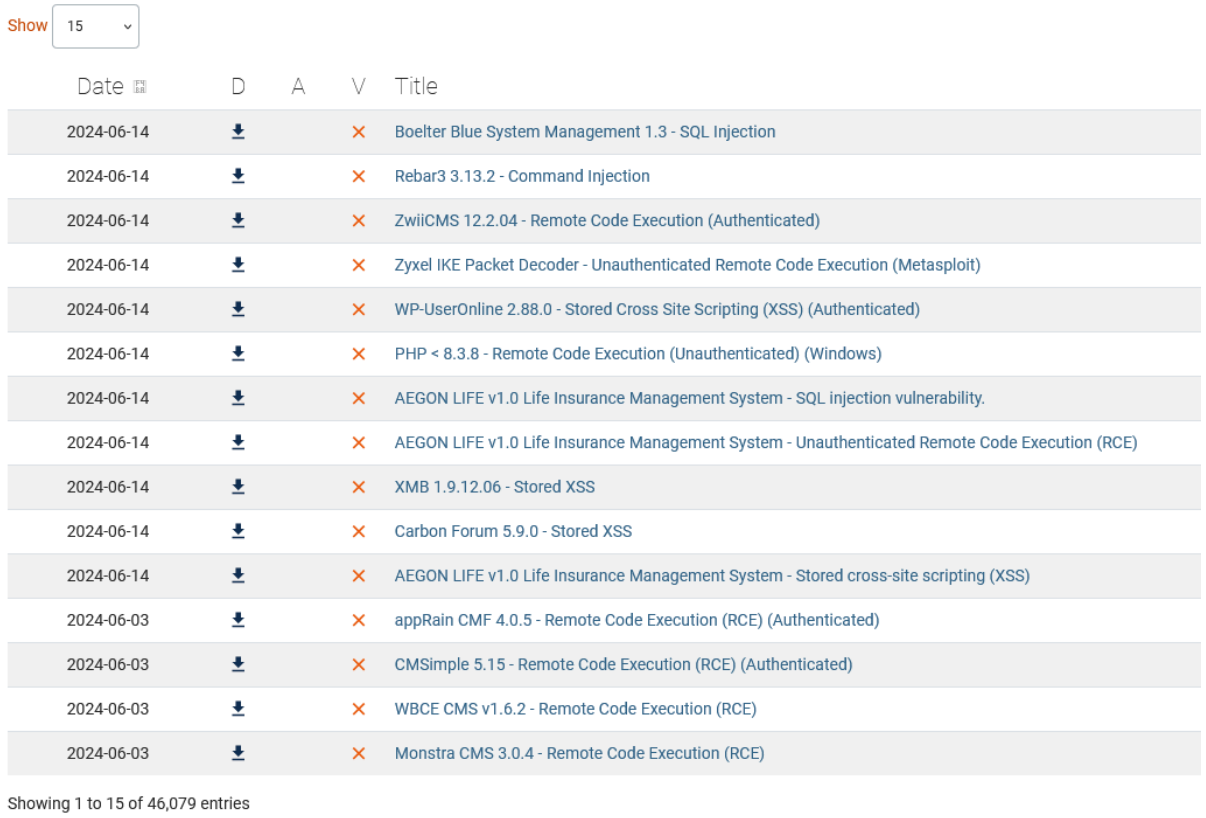
5.2 Scanning

La prochaine étape consiste à utiliser toutes les informations recueillies pour évaluer les potentielles vulnérabilités.

Par exemple, si un ordinateur exécute un serveur FTP nommé vsftpd version 2.3.4, une recherche dans des bases de données spécialisées peut révéler que cette version est vulnérable à une faille RCE (Remote Code Execution).

Cela signifie qu'il est possible d'exécuter du code à distance sur la machine vulnérable.

Cependant, trouver une faille ne signifie pas que le travail est terminé. Il pourrait y avoir d'autres vulnérabilités, potentiellement plus graves, ailleurs dans le système.



5.3 Exploitation

Une fois les vulnérabilités identifiées, il faut les exploiter pour obtenir ce que l'on veut (par exemple, un accès au serveur).

Cette phase permet de confirmer que les vulnérabilités sont bien réelles.

5.4 Post-exploitation

Les phases suivantes peuvent être optionnelles et dépendent du type de test et des failles trouvées.

Par exemple, si vous obtenez un accès à distance au serveur (obtenir un shell), vous pouvez insérer une porte dérobée (une backdoor en anglais) pour y accéder plus tard.

5.5 Nettoyage des traces

Lors de l'exploitation des vulnérabilités, des traces sont laissées (logs, fichiers, trafic réseau, etc.). Ces traces peuvent être utilisées par des analystes SOC pour détecter une attaque et réagir en conséquence. Le but de cette étape est de nettoyer toutes les traces de l'attaque pour rendre la tâche difficile aux défenseurs.

Attention à ne pas causer de dommages aux systèmes cibles, surtout si l'infrastructure testée est en production. (par exemple il faut faire attention à ne pas supprimer ou altérer la base de donnée du client)

Il y a des règles à respecter pour éviter des conséquences indésirables.

Une fois l'attaque simulée et les vulnérabilités identifiées, il est crucial de communiquer ces failles de sécurité au client à l'aide d'un rapport.

Ce rapport doit lister toutes les failles de sécurité, leur gravité et les recommandations pour y remédier.

C'est une phase très importante car le rapport peut être la seule chose que le client verra à la fin. Le rapport doit donc être aussi clair et détaillé que possible sur les problèmes techniques identifiés.

6. Quelles sont les compétences techniques de base à maîtriser ?

Apprendre à tester et à protéger un système d'information ne s'improvise pas du jour au lendemain.

Pour mettre en œuvre tout ce dont je vous ai parlé, il est nécessaire de posséder des compétences avancées en informatique, notamment sur le fonctionnement des systèmes, des réseaux, des vulnérabilités, etc.

Si un professionnel manque de connaissances, cela peut avoir de graves répercussions financières pour l'entreprise. Par exemple, pour comprendre comment "hacker" un site web, il est essentiel de comprendre d'abord le fonctionnement des sites web. De même, pour auditer le code d'une application et vérifier sa sécurité, il est indispensable de maîtriser la programmation.

Il peut sembler évident que de nombreux débutants se lancent directement dans des tâches avancées, comme l'utilisation d'outils de sécurité informatique sous Kali (tels que Wireshark, Hashcat, Hydra, Burp Suite, etc.), sans réellement comprendre leur fonctionnement.

Pour pratiquer la sécurité informatique de manière efficace, il est donc impératif de posséder une solide base en informatique.

Heureusement, j'ai dressé une liste des cinq compétences techniques essentielles que vous devez apprendre :

6.1 La programmation

Savoir programmer, c’est savoir donner des ordres à une machine grâce au code et automatiser des tâches.

Tout ce que tu fais manuellement avec la souris, tu pourras le faire en tapant des lignes de code, et ce, 100 fois plus vite. Il est donc essentiel de maîtriser la programmation.

Cependant, tu n’as pas besoin de devenir le meilleur développeur dans tous les langages de programmation. Ce n’est pas nécessaire. En revanche, tu dois être capable d’écrire des scripts (des petits bouts de code) pour atteindre tes objectifs, comme par exemple :

- Envoyer un paquet réseau avec une IP usurpée (spoofée en anglais).
- Envoyer le même paquet 50 fois par seconde.
- Décoder une chaîne de caractères en base 64, extraire les 5 premiers caractères et appliquer le chiffrement AES dessus.
- Créer un malware qui envoie tous les mots de passe du navigateur chaque jour à 17:50.

Toutes ces tâches sont impossibles à réaliser manuellement (cela prendrait trop de temps) et ne peuvent pas non plus être accomplies simplement en utilisant un logiciel (c’est moins précis et moins personnalisable).

Les deux langages de programmation les plus simples pour débuter sont Python (un langage polyvalent) et JavaScript (principalement utilisé dans le web). Cependant, il existe de nombreux autres langages avec des cas d’usage différents (web, Android, iOS, Windows).

L’avantage est qu’une fois que tu connais 2 ou 3 langages de programmation, tu pourras en apprendre n’importe lequel à la demande, car la plupart des langages de programmation partagent des bases communes.

Mais concentre-toi d’abord sur un seul.

6.2 Les réseaux

Maîtriser le fonctionnement des réseaux, c'est comprendre comment les ordinateurs communiquent entre eux.

Pour que les ordinateurs puissent communiquer, ils doivent parler la même langue (un peu comme les humains).

La plupart du temps, les ordinateurs communiquent en utilisant le modèle TCP/IP, qui est la langue commune regroupant des protocoles tels que IP, TCP, Ethernet, UDP, HTTP, etc.

C'est également l'un des piliers essentiels à connaître.

6.3 Maîtrise de linux

Beaucoup de systèmes informatiques à sécuriser fonctionnent sous Linux. La plupart des outils de sécurité informatique fonctionnent mieux sous Linux.

De manière générale, il est plus facile de bidouiller Linux que Windows ou Mac, ce qui offre une plus grande liberté pour effectuer diverses actions.

Cependant, si vous utilisez Windows ou Mac, vous n'êtes pas obligé de supprimer votre système actuel pour installer Linux. Vous pouvez plutôt :

- Installer VirtualBox ou VMware, qui sont des hyperviseurs permettant de simuler un PC à l'intérieur d'un autre PC (appelé machine virtuelle). : https://www.virtualbox.org/
- Installer Linux (Debian, Kali, Ubuntu) dans la machine virtuelle.
- Utiliser toutes les fonctionnalités de Linux directement à partir de Windows ou de Mac.

Maîtriser linux est donc indispensable 🙂

6.4 Maîtrise des protocole web

Pour accéder à internet, comment fais-tu ?

Oui, tu ouvres ton navigateur (Chrome, Firefox ou autre), tu fais une recherche, puis tu visites le site de ton choix.

Le problème est que de nombreux sites internet possèdent des failles de sécurité, et une partie importante de la demande en cybersécurité concerne la sécurisation des services et des applications web.

Il est donc primordial d'apprendre comment fonctionne le web, ce qui comprend :

- Les langages web comme HTML et CSS
- Les langages de programmation côté serveur ou côté client (comme PHP et JavaScript)
- Le fonctionnement des protocoles web comme HTTP
- Etc.

Cette connaissance est essentielle pour identifier et corriger les vulnérabilités, assurant ainsi la sécurité des utilisateurs et des données.

6.5 Fonctionnement bas niveau d’un ordinateur

Que penses-tu de la signification du terme "informatique" ?

L'informatique est définie comme la "science de l'information". Rien de plus.

Depuis les années 80, avec le début de la révolution numérique, nous avons pu traiter et transférer l'information à une vitesse incroyable !

Comment l'information est-elle représentée dans un ordinateur ? Elle est représentée en binaire : tout, que ce soit des photos, des vidéos, du texte,

des programmes ou le système d'exploitation Windows, n'est qu'une suite de 0 et de 1.

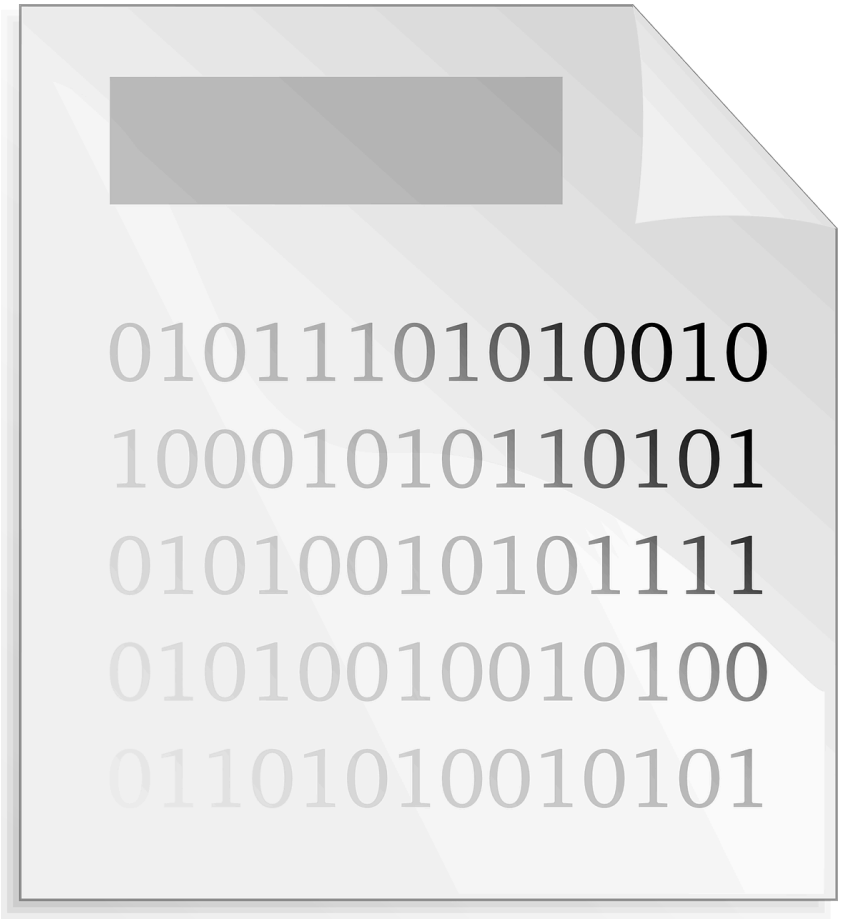
Cela peut être une suite très longue, mais tout revient à ces deux chiffres. Par exemple, une vidéo de 1 Go est simplement une suite de 8 milliards de 0 ou 1 (c’est-à-dire 8 milliards de chiffres binaires).

Comme tu l'as deviné, l'informatique se résume à des 0 et des 1. L’ordinateur ne peut traiter que des 0 ou des 1, rien d’autre.

Le reste n'est donc qu'une question d'abstraction.

Pour bien débuter, il est crucial de maîtriser le binaire (ainsi que l'hexadécimal, qui est une forme condensée du binaire).

Il est également important de comprendre le fonctionnement du processeur, de la mémoire RAM et des différents composants d'un ordinateur.



7. Quelles sont les erreurs à éviter ?

7.1 Faire trop de “CTFs”

Pour ceux qui ne le savent pas, un CTF (Capture the Flag, ou "capturer le drapeau" en français) est un ensemble de mini-challenges de sécurité informatique. Le but est de "hacker" des systèmes, un peu comme des casse-têtes informatiques.

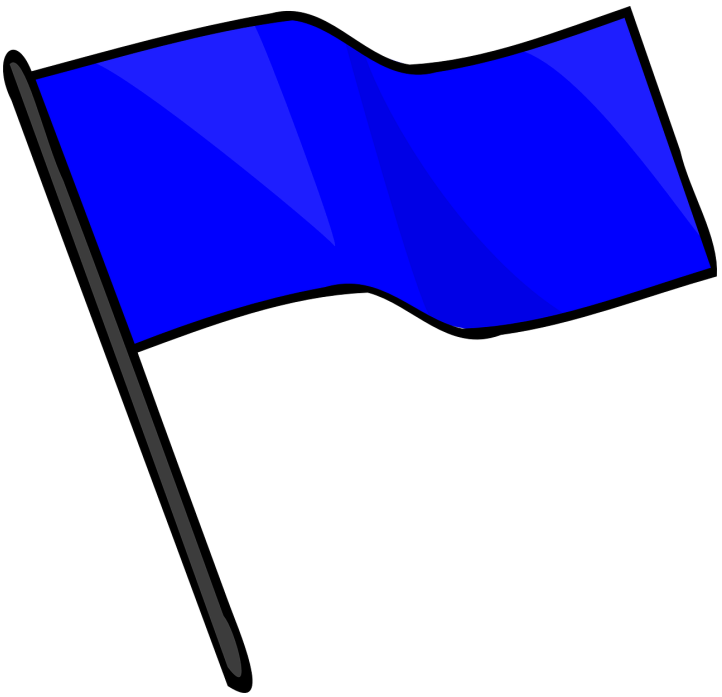
Comment cela fonctionne :

1. Vous déployez une machine vulnérable à une faille de sécurité
2. Vous essayez de hacker cette machine et de trouver la faille de sécurité
3. Quand vous avez exploité la faille de sécurité, vous avez accès à “un drapeau” ou un “flag” (en anglais) qui prouve que vous avez exploité la faille donc réussi le “casse-tête”

Le problème des CTF, c’est que

- Ils sont destinés à des étudiants ayant déjà de bonnes bases en cybersécurité pour comprendre les différents types d’attaques. Donc, si tu n’as pas les bases en informatique, ne fais surtout pas de CTF, car tu ne comprendras rien.
- Être bon en CTF ne signifie pas être non plus bon dans le monde professionnel. Car les failles de sécurité dans les “challenges” CTF ne ressemblent pas toujours aux failles de sécurité que tu vas rencontrer en pratique dans les entreprises.
- De plus, de nombreuses plateformes de CTF vous font pratiquer des failles de sécurité qui ne sont plus présentes aujourd’hui.

Donc, ne fais pas uniquement des CTF même si c’est une bonne manière de pratiquer certains types d’attaque.



7.2 Faire plein de projets en même temps

Quand je lis vos messages et que j’accompagne mes élèves, j’ai remarqué que beaucoup d’entre vous se dispersent trop, c'est-à- dire apprennent plein de "trucs" en même temps. Si c'est ton cas, cela montre que tu es curieux, et c'est une qualité !

Mais, par pitié, ne te lance pas dans dix projets différents en même temps.

À la fin, c'est la catastrophe. Tu te fatigues plus vite et tu te sens dépassé. Tu ne finis rien (ou tu fais tout à moitié). Tu oublies beaucoup plus facilement ce que tu as fait, car le cerveau humain n'est pas fait pour travailler sur plusieurs projets au cours de la journée.

Concentre-toi sur un seul projet ou un seul cours et finis-le ! C’est dix fois mieux que de commencer dix choses différentes sans les terminer. Ce conseil peut paraître évident pour certains, c'est vrai. Mais je parie que peu de gens l'appliquent vraiment...

7.3 Passer trop de temps à faire de la théorie

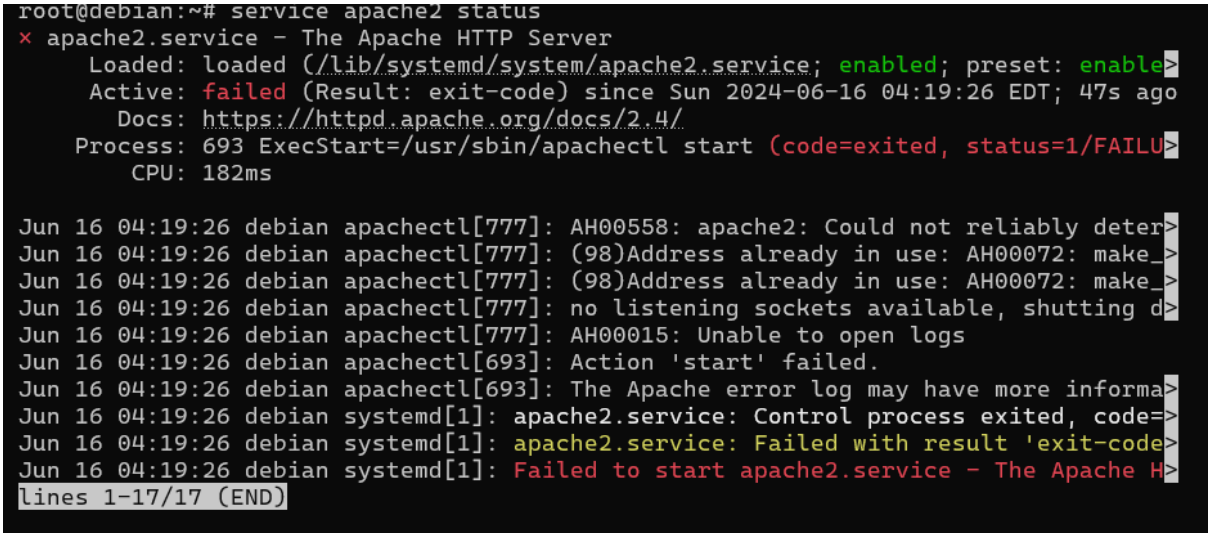
Je constate souvent lors de mes accompagnements que mes élèves regardent des vidéos techniques sans prendre le temps de pratiquer ce qu'ils y apprennent.

Cela peut être une vidéo sur l'installation d'un serveur web Apache (Apache est un serveur qui gère environ 30 % des serveurs web dans le monde).

Le problème est qu'il est facile de regarder une vidéo expliquant comment installer un serveur web Apache. On a alors l'impression d'être productif.

Cependant, la pratique est une tout autre histoire. En pratiquant, tu te confrontes à des problèmes que tu n'avais pas anticipés et qui ne sont peut-être pas abordés dans le tutoriel "Comment installer un serveur Apache", tels que :

- une erreur dans un fichier de configuration,
- le service Apache qui ne démarre pas,
- des problèmes de permissions des dossiers auxquels Apache doit accéder,
- la machine virtuelle qui n'arrive pas à se connecter au PC hôte,
- etc...



Et 80 % de ton apprentissage se fera en résolvant ces problèmes, tout simplement.

C'est-à- dire en regardant les logs, en isolant les problèmes, en testant une autre solution etc...

Malheureusement, comme il est plus difficile de pratiquer et de résoudre ces problèmes, les débutants préfèrent simplement regarder les vidéos, car c'est plus facile et cela donne l'impression d'être tout aussi productif.

Voici la règle que tu dois appliquer à partir de maintenant : Si tu regardes une vidéo technique, comme un tutoriel, considère que tu ne l'as pas vraiment regardée tant que tu n'as pas pratiqué et terminé ce qu'elle enseigne.

C'est aussi simple que cela.

8. Quelles sont les différents types d'attaques

Les métiers dans la cybersécurité ne se limitent pas au piratage ou à l'intrusion dans le système de quelqu'un d'autre.

Lorsque vous êtes embauché par une entreprise, cela signifie que vous répondez à un besoin spécifique : le besoin de sécurité de l'entreprise.

Votre objectif est de protéger l'entreprise contre tous les types de risques.

Dans cette partie, j'aimerais vous présenter les types d'attaque les plus courantes :

8.1 Attaque DOS

DOS signifie "denial of service" ou "déni de service". Le but d'une attaque DOS n'est pas de prendre le contrôle de l'infrastructure de la victime, mais de la rendre indisponible.

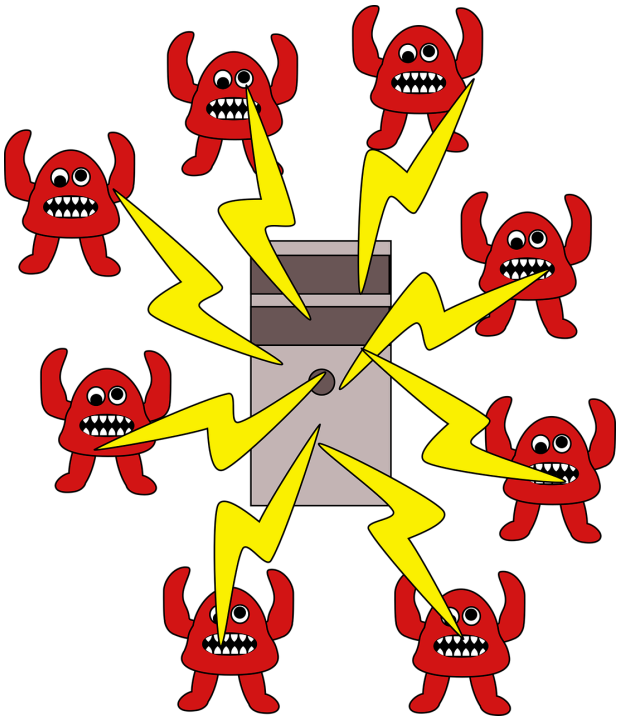
Il y a plusieurs façons d'y parvenir :

- Submerger le service de requêtes jusqu'à saturation
- Faire planter le service en exploitant une erreur de programmation
- Supprimer toutes les données de la base de données
- Installer un rançongiciel (qui chiffre toutes les données avec une clé secrète et demande de l'argent en échange de cette clé pour déchiffrer les données sensibles)
- Etc.

8.2 Attaque DDOS

DDOS signifie Distributed Denial of Service, ce qui est similaire à une attaque DOS mais réalisé de manière groupée avec plusieurs attaquants tentant de submerger le système de la victime avec des requêtes.

Il est important de faire la différence entre DOS et DDOS.



8.3 Espionnage

Souvent, le but d'une attaque est d'espionner la cible afin d'en tirer des informations sensibles telles que des bases de données, des clés de chiffrement, des fichiers, des activités, des secrets industriels, des mots de passe, etc.

Il y a plusieurs manières d'atteindre cet objectif.

La méthode la plus directe est d'exécuter du code sur la machine de la victime.

Une fois que l'attaquant a exécuté du code, il pourra y installer un malware (un logiciel malveillant en anglais) qui espionnera la victime.

8.4 Ingénierie sociale

Si le système informatique ne présente pas de failles apparentes, une autre méthode pour accéder à ce système est de passer par un humain qui possède déjà les accès nécessaires.

Par exemple, si je veux obtenir le mot de passe Google de ma cible, je pourrais rediriger la cible vers un site qui ressemble à Google (et ainsi me faire passer pour Google), afin que la cible saisisse ses identifiants sur mon site. À partir de là, je pourrais les récupérer sans difficulté.

Cette attaque est appelée "phishing", et il existe des dizaines de variantes encore plus sournoises les unes que les autres.

9. Maîtriser Les “soft-skills”

Dans les métiers (pas seulement dans l'informatique), il y a en général deux types de compétences :

1. **Les hard skills** Ce sont l'ensemble des compétences techniques (savoir faire un test d'intrusion, savoir développer un site web, répondre à un incident, etc.).
2. **Les soft skills** Ce sont toutes les compétences relationnelles, c'est-à-dire communiquer ses résultats, écrire des rapports, savoir travailler en équipe, etc.

Les hard skills, c’est évident, vous devez les connaître pour bien faire votre travail cependant :

Ne négligez jamais les soft skills, même si vous êtes dans un domaine très technique comme la cybersécurité.

Par exemple, si vous êtes pentester, le rapport que vous livrez au client est destiné à un humain qui n'a peut-être pas les mêmes compétences que vous. Vous devez donc savoir vous mettre à la place du client et adapter votre niveau de langage.

Plus généralement, n'oubliez pas qu'on ne vous embauche pas pour faire un tas de choses abstraites, mais plutôt pour résoudre un problème précis pour le client.

10. Conclusion

Vous avez tout ce qu’il vous faut pour démarrer dans la cybersécurité

je n’ai pas voulu faire ce guide trop long pour ne pas vous surcharger d’informations.

En tout cas, j’espère que ce guide vous as plus 🙂