



Bonjour, je vais essayer de répondre à la question "[Quelle devrait être ma feuille de route en matière de cybersécurité ?](#)", qui est une question que je rencontre très souvent dans mon poste actuel.

D'ailleurs, vous pouvez modifier légèrement les parties dans cet ordre en fonction de votre propre style d'apprentissage.

Bonne lecture.



Apprendre une langue



La chose à laquelle les personnes qui se lancent dans la cybersécurité devraient accorder le plus d'attention et qu'elles devraient apprendre en premier lieu est l'apprentissage de la langue.

La première raison en est le manque d'échange d'informations dans notre pays.

Bien que des sites comme celui-ci partagent des informations sur ce domaine, ils ne sont malheureusement pas suffisants.

Nous devons connaître la langue, en particulier pour suivre et apprendre les nouvelles vulnérabilités et failles.

[Quelles sont donc les langues que nous devons apprendre pour la cybersécurité ?](#)

1. l'anglais

De nombreux articles et contenus écrits dans le domaine de la cybersécurité sont rédigés principalement en anglais, car il s'agit d'une langue internationale.

Par conséquent, la première langue que nous devons apprendre lorsque nous nous lançons dans la cybersécurité est l'anglais.

2. le russe

La Russie est l'un des pays les plus en vue dans le domaine de la cybersécurité aujourd'hui.

Il y a donc un partage excessif des ressources et une abondance de ressources.

Il est également indiqué que de nombreuses ressources importantes sont disponibles en russe.

3. chinois

Même s'il n'est pas aussi facile à apprendre que les deux autres langues, le chinois est une langue qui sera très utile dans ce domaine.

La Chine étant l'un des pays du monde où les cyberattaques sont les plus nombreuses, il existe de nombreuses ressources en matière de cybersécurité en chinois.

En outre, l'apprentissage de l'allemand et du français peut vous être utile.



Apprendre les systèmes d'exploitation



L'apprentissage des systèmes d'exploitation et de leur logique de fonctionnement vous permettra de faire un pas de plus en matière de cybersécurité.

En particulier, la connaissance des commandes de terminal vous donnera un avantage lors de l'utilisation du système d'exploitation et de l'infiltration d'appareils à l'avenir.

Quels sont donc les systèmes d'exploitation que nous devons apprendre à utiliser pour la cybersécurité ?

1. Kali Linux

Ce système d'exploitation, dont ceux qui se sont lancés ou se lanceront dans la cybersécurité ont entendu parler au moins plusieurs fois, est, à mon avis, le meilleur système d'exploitation que vous puissiez utiliser pour la cybersécurité.

Si l'on considère à la fois les performances, la conception et la facilité d'utilisation, on constate que Kali Linux est l'un des meilleurs systèmes d'exploitation.

De plus, si l'on considère que le but du développement de ce système d'exploitation est le pentest, on voit qu'il surpasse de nombreux systèmes d'exploitation.

Site web : [Kali Linux - Distribution Linux pour le test de pénétration et le piratage éthique](#)

2) Parrot Os

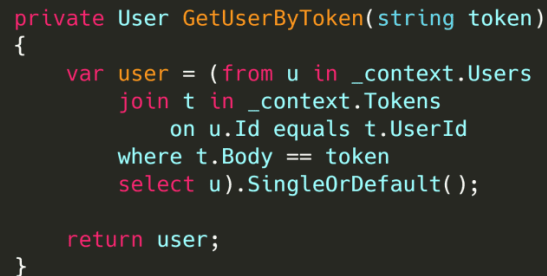
Comme Kali Linux, ce système d'exploitation a été spécialement créé pour le pentest.

En outre, la conception visuelle de certains outils fait que ce système d'exploitation se distingue, en particulier pour les débutants.

Site web [Parrot Security](#)

Outre ces deux systèmes d'exploitation, d'autres systèmes d'exploitation devraient être examinés : [BlackArch](#), [Windows](#), [Tails](#), [Whonix](#).

Apprendre les bases de la programmation



```
private User GetUserByToken(string token)
{
    var user = (from u in _context.Users
                join t in _context.Tokens
                  on u.Id equals t.UserId
                where t.Body == token
                select u).SingleOrDefault();

    return user;
}
```

Quels sont donc les langages logiciels que nous devons apprendre pour la cybersécurité ?

1) Python

Le langage Python, qui est un langage que je n'aime pas beaucoup personnellement, est préféré parce qu'il est facile à apprendre et qu'il dispose de beaucoup de ressources.

2) PHP

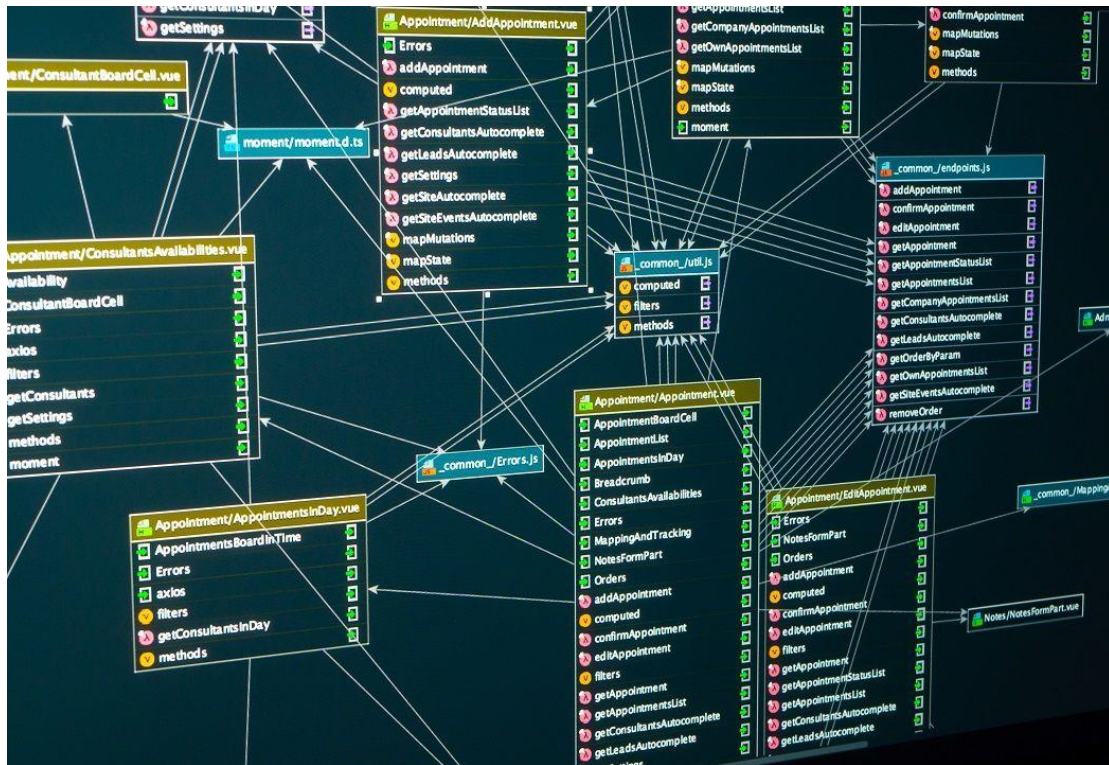
Ce langage, qui fonctionne sur les serveurs web, est un langage que ceux qui travailleront dans le domaine web de la cybersécurité doivent absolument connaître.

3) JavaScript

Ce langage, qui est également utilisé dans le domaine du web, doit être appris car il est présent dans la plupart des sites web et provoque des vulnérabilités.

Voici quelques langages que vous pouvez apprendre en plus de ceux mentionnés ci-dessus : [C++](#), [Ruby](#), [C#](#), [Java](#).

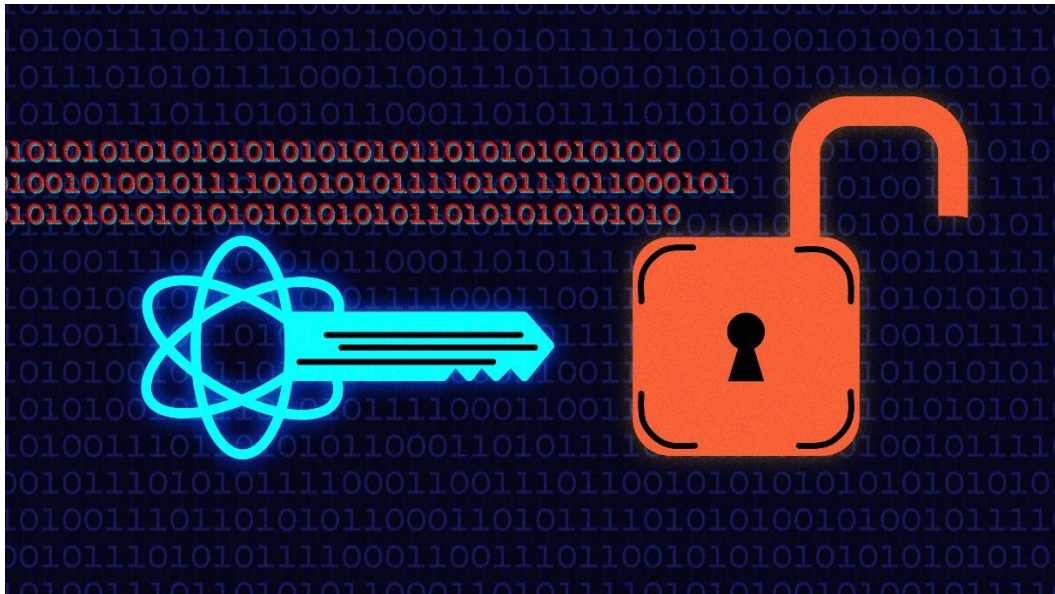
Apprendre la structure d'une base de données



Connaître la logique de fonctionnement de la structure de la base de données vous donnera un avantage au moment de l'attaque ou du test.

De cette manière, vous connaîtrez la détection de l'attaque, la cause et les précautions des vulnérabilités existantes.

Apprendre les structures de cryptage



Connaître les structures de cryptage vous aide à protéger vos systèmes et vos mots de passe.

Quelles sont donc les structures de cryptage que nous devons apprendre pour la cybersécurité ?

1) Aes

La méthode de cryptage Aes a pour caractéristique de crypter vos données avec des systèmes de 128-196-256 bits.

Elle crypte vos données principales en fonction des valeurs **IV et Key** données et ne peut pas être restaurée sans ces **valeurs IV et Key**.

2) Des

La méthode de cryptage Des est similaire à la méthode de cryptage Aes.

Là encore, elle crypte vos données à l'aide de l'**IV et de la CLÉ** et ne peut être décryptée sans l'**IV et la CLÉ**.

3) MD5

Contrairement aux deux autres méthodes, cette méthode de cryptage n'est pas cryptée à l'aide de l'IV et de la clé, et elle ne peut pas être restaurée car il s'agit d'un cryptage unilatéral.

Elle convertit également en un mot de passe de 32 caractères, quelle que soit la valeur donnée.

Il existe également des versions antérieures telles que MD2-MD4.

4. LE SHA256

SHA256, qui est également une méthode de chiffrement populaire, est chiffré unilatéralement comme MD5 et ne peut pas être restauré.

Il ne nécessite pas non plus d'IV et de clé comme MD5. La différence par rapport à la structure MD5 est sa longueur.

Alors que MD5 se compose de 32 caractères, SHA256 se compose de 64 caractères.

On peut également utiliser SHA1, SHA224, SHA384, SHA512.

Apprendre le matériel informatique et la logique de fonctionnement



Bien qu'il ne soit pas aussi important que d'autres éléments, il est utile d'apprendre à connaître les pièces d'un ordinateur et son fonctionnement.

Les principaux systèmes que vous devez apprendre ;

Carte mère

Processeur

Carte vidéo

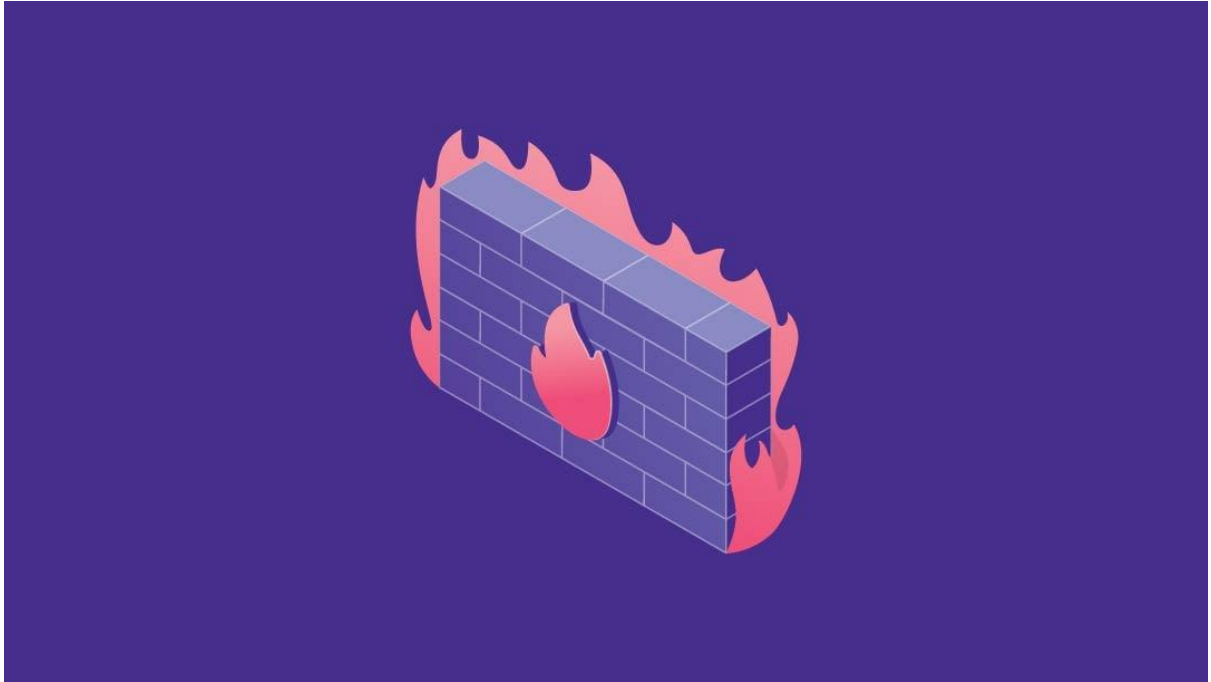
Ram

SSD

Disque dur

Bloc d'alimentation

Apprendre les pare-feu



Étant donné que les pare-feu permettent d'éliminer de nombreuses cyberattaques et menaces, il est important que le responsable de la cybersécurité sache comment les installer et les utiliser.

Apprendre les méthodes de cyberattaque



Un spécialiste de la cybersécurité, c'est-à-dire un hacker "white hat", doit également connaître les méthodes "black hat" pour arrêter/bloquer/tester les attaques.

C'est pourquoi

Injection SQL

logiciel malveillant

Brute Force

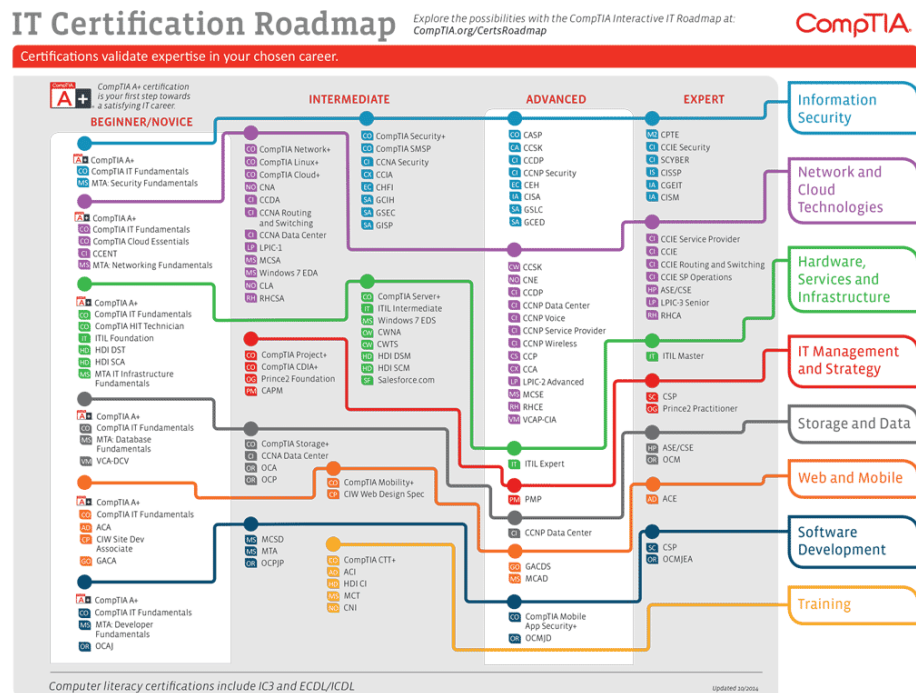
XSS

CSRF

Ransomware

Vous devez apprendre des méthodes telles que ceux la .

Obtenir un certificat



Notre dernier point sera d'obtenir un certificat lié à notre domaine.

Ces certificats nous permettront d'évoluer dans notre domaine et vous donneront un avantage lors de la recherche d'un emploi.

Voici quelques exemples de ces certificats ;

CompTIA Security + (sécurité)

Professionnel certifié de la sécurité des systèmes d'information (CISSP)

Hacker éthique certifié (CEH)

Gestionnaire certifié de la sécurité de l'information (CISM)

Professionnel certifié en sécurité offensive (OSCP)

Enfin, je laisse ici quelques ressources sur la cybersécurité, que vous pouvez également consulter.

[Ressources pour s'initier à la cybersécurité](#)

Propriétaire du sujet Ben

[Recommandations pour la cybersécurité | Monté sur genou](#)

[Qu'est-ce qu'un réseau \(LAN - WLAN - VPN - Caractéristiques générales\) ?](#)

[Qu'est-ce que le certificat CEH ?](#)

[Collecte d'informations actives et passives \(DÉTAILLÉ \)](#)

[Mes livres/recommandations sur le sujet](#)

[Sécurité de l'information avec PowerShell \(Dossier\)](#)

[Systèmes d'exploitation personnalisés - Sécurité, confidentialité, piratage](#)

Voici brièvement notre feuille de route. J'espère qu'elle sera utile aux débutants.

Bons forums.

TURKHACKTEAM.ORG