# Roadmap Pentest by tatsu

Bonjour, je suis Tatsu, **étudiant en cybersécurité**, et je fais cette roadmap pour la simple et bonne raison que des amis ou même des gens m'ont demandé comment j'ai fait pour arriver à un tel niveau. Alors, dans cette roadmap, je vous donne **tout ce dont vous avez besoin** pour **arriver à mon niveau, voire plus** ! Cette roadmap sera **divisée en trois grandes parties** : **1. Le commencement, 2. L'apprentissage (jusqu'à arriver à mon niveau), 3. Quelle est la prochaine étape** ?

## 1. Le commencement

Pour bien commencer, vous devez être sûr d'avoir **installé Obsidian.**
Obsidian est un outil qui vous permettra de **prendre des notes** de manière **propre** et même de **les transformer en PDF**. Car oui, **prendre des notes est sûrement l'une des choses les plus importantes quand on apprend la cybersécurité**. Il y a tellement de choses à apprendre... Imaginez : vous êtes en CTF, vous ne vous souvenez plus d'une faille que vous avez vue mais que vous n'avez pas notée. Vous allez passer des heures à la chercher, alors qu'avec des notes, il suffit de les consulter.

Après avoir installé Obsidian, vous devez **installer Kali Linux**. C'est une **distribution de Linux** spécialement **conçue pour la cybersécurité**. Voici un tutoriel pour l'installer :
https://www.youtube.com/watch?v=9gHa1w-JAkw

Ensuite, créez un compte sur le site https://Tryhackme.com.
Ce site regorge de"rooms" qui vous **permettront d'apprendre** et de vous **entraîner en CTF.**

Maintenant que vous avez Obsidian, vous pouvez **commencer à apprendre** ! Voici un ordre qui vous permettra d'**apprendre** de manière **optimisée**, sans perdre trop de temps.

- Regardez quelques vidéos de personnes faisant des CTF pour voir à quoi cela ressemble (voici quelques vidéos) :
  https://www.youtube.com/watch?v=ZCuStkgjwM8
  https://www.youtube.com/watch?v=Oye_mAxslqA
  https://www.youtube.com/watch?v=b3deYs4LPuI

- Je vous **recommande** surtout les vidéos de personnes faisant du **bug bounty** (en gros, des entreprises comme Nike, Adidas, Temu, etc., proposent sur des sites comme https://hackerone.com de trouver des failles contre de l'argent). Ces vidéos sont **remplies de conseils** à intégrer dans votre propre pratique. Voici **deux bonnes chaînes YouTube sur le bug bounty** :
  https://www.youtube.com/@HackShiv
  https://www.youtube.com/@the_cyb3rb0y
- Ensuite, faites les "rooms" **Linux Fundamentals Part 1, 2 et 3 sur TryHackMe.** Les parties 2 et 3 sont en premium, mais vous pouvez accéder aux contenus ici :
  https://electronicsreference.com/thm/linux_fundamentals_pt2/
  https://electronicsreference.com/thm/linux_fundamentals_pt3/
- Après avoir fait ces trois rooms et pris des notes, faites **les rooms de base de TryHackMe**, à savoir :
  https://tryhackme.com/r/room/introtooffensivesecurity
  https://tryhackme.com/r/room/cyberkillchainzmt
  https://tryhackme.com/r/room/securityprinciples
  https://tryhackme.com/r/room/httpindetail
  https://tryhackme.com/r/room/howwebsiteswork
  https://tryhackme.com/r/room/pentestingfundamentals
  https://tryhackme.com/r/room/redteamfundamentals
  https://tryhackme.com/r/room/furthernmap Oui, il y a énormément de choses, mais ce sont toutes des connaissances essentielles. Par exemple, la cyberkill chain : si vous ne la connaissez pas, vous ne dépasserez jamais l'étape de Nmap et Gobuster dans un CTF.
- Après cela, je pense que vous aurez le niveau pour **faire vos premiers CTF.** Voici **quatre CTF** dans l'**ordre de difficulté croissante** :
  https://tryhackme.com/r/room/rrootme
  https://tryhackme.com/r/room/picklerick
  https://tryhackme.com/r/room/cyborgt8
  https://tryhackme.com/r/room/mrrobot

## 2. L'apprentissage

Bien, vous avez maintenant fait vos premiers CTF, vous connaissez toutes les commandes de base de Linux, mais ce n'est pas suffisant, vous en voulez plus, bien plus.

Pour continuer votre apprentissage, je vous offre un livre de plus de 300 pages sur la cybersécurité. "Apprendre l'attaque pour mieux se défendre " C'est un **excellent livre** en français. LISEZ CE LIVRE ABSOLUMENT. Il vous apprendra facilement **dix fois plus** que les rooms TryHackMe ou des vidéos YouTube. vous pouvez lire le livre ici https://repo.zenk-security.com/Magazine%20E-book/Securite%20Informatique%20-%20Ethical%20Hacking.pdf

Bien sûr, vous **prenez des notes** pendant la lecture. En plus du livre, continuez à **regarder des vidéos de bug bounty** et à vous **entraîner** avec des **CTF** ou des **KOTH**. Vous apprendrez énormément.

## 3. Quelle est la prochaine étape ?

Sachez que si vous êtes arrivé à ce stade, vous êtes à mon niveau en cybersécurité. Mais alors, quelle est la prochaine étape pour progresser ? Vous devrez simplement **apprendre l'anglais** et lire des livres. Malheureusement, la **plupart des livres ou vidéos parlant de cybersécurité sont en anglais**. Le livre que je vous ai recommandé **est une rare exception**.

Une autre façon d'apprendre est de **continuer à pratiquer**. Quand vous arrivez à un niveau où vous réussissez des CTF difficiles, même si vous n'y parvenez pas au début, regardez des vidéos de personnes faisant des CTF difficiles, prenez des notes sur les choses importantes, et refaites la CTF. Vous atteindrez sûrement un point où les CTF TryHackMe seront **trop simples** ou qu'il en restera trop peu à faire. Vous passerez alors à une autre plateforme : https://www.hackthebox.com, qui propose de nombreuses nouvelles CTF, et celles-ci sont plus difficiles que celles de TryHackMe. Vous apprendrez donc encore plus.

Quand vous atteindrez un certain niveau sur HackTheBox, vous changerez de plateforme pour aller sur https://www.root-me.org. Non seulement Root-Me est **encore plus difficile**, mais c'est aussi **en français** !

Voilà, je vous ai donné ma propre roadmap pour apprendre la cybersécurité. Vous n'avez plus qu'à vous lancer ! N'oubliez pas que peu importe le niveau de difficulté que cela peut représenter pour vous, n'abandonnez jamais. On peut toujours apprendre. Personne n'est bloqué. Peut-être que vous mettrez plus de temps à apprendre quelque chose, mais que vous comprendrez une autre notion en 30 minutes.

Par exemple, je n'arrivais pas à comprendre ce qu'était un tunnel SSH et à quoi il servait. J'ai passé une semaine à chercher, j'ai même appelé un pote pour en parler, et finalement, même si cela m'a pris du temps, j'ai fini par comprendre comment sa marchais **Faites pareil : n'abandonnez pas**.