

COMMENT DEVENIR UN EXPERT EN SECURITE INFORMATIQUE EN QUELQUES MOIS ?

Ce livre est un guide pour vous permettre de devenir rapidement des professionnels de la sécurité informatique.

Ce livre a été écrit pour tous les niveaux et grâce à mon père biologique.



MAIZAN KOUAME MELCHISEDEK

Consultant, Ecrivain, Pentester

Sommaire :

- I. Introduction
- II. Les principes
- III. Loi ultime
- IV. Expert en sécurité système
- v. Où trouver son inspiration ?

I/ Introduction

La sécurité informatique est un domaine assez vaste comparable à la médecine, elle a en son sein plusieurs spécialités. Les spécialités en informatique sont :

Testeur d'intrusion, **Architecte** de sécurité, **Conseiller** en sécurité de l'information, **Conseiller** en prévention fraude, **Spécialiste** en réponse aux incidents, **Analyste** en surveillance réseau.

Dire que je suis un expert en sécurité informatique signifie qu'on est comme un généraliste en médecine.

Vu sous cet angle, vous devez alors avoir une spécialité pour devenir un expert dans le domaine vaste de la sécurité informatique. Alors on peut se poser la question suivante : quelles sont les principes fondamentaux à respecter pour devenir un expert dans une spécialité choisie en informatique ?

II/ Les principes fondamentaux d'une spécialité en sécurité informatique

Les principes ici sont des conseils par expérience et par observation ; ceux-ci sont donnés pour permettre à tous ceux qui sont dans la sécurité informatique d'ouvrir les yeux et aussi d'avoir une idée et une vision claire ainsi que des méthodes pratiques pour vite évoluer et exceller dans un domaine qu'on aurait choisi.

A. Premier Principe : S'avoir ce qu'on veut.

S'avoir ce qu'on veut, veut tout simplement dire que vous devez avoir une vision claire de ce que vous voulez devenir précisément ou dans quelle compétence avoir une expertise en sécurité informatique. Ne soyez pas dans « tout » à la fois. Vous risquez de ne rien maîtriser car le hacking dans chaque spécialité regorge beaucoup de choses. Ce qui veut dire que vous devez d'abord avoir une vision de ce que vous voulez de sorte à avoir une passion.

B. Deuxième Principe: Avoir une passion.

La passion : Affection, intérêt très vif pour quelque chose. L'objet de cette affection. Exemple : Avoir une passion pour le sport. Amour intense.

Avoir une passion pour ce que vous désirez faire est très important, car ça sera le premier moteur que vous allez utiliser pour avancer dans un domaine ou dans une spécialité. Notez que sans cela il vous sera difficile de démarrer ou de déboursier de l'argent pour acquérir la connaissance qu'il faut dans ce domaine.

La passion a même la capacité de créer en vous une discipline à force de travailler sur vos cours et outils de cyber attaque et de cyber défense.

C. Troisième Principe: Etre discipliné

La discipline : La discipline est l'ensemble des règles de conduite communes imposées aux membres d'un groupe, d'une collectivité, d'une organisation sociale, d'un ordre, d'une armée, etc. afin d'y faire régner l'ordre et de garantir son bon fonctionnement.

La discipline est l'art même d'atteindre le sommet. Je veux dire par là que si vous avez dans la journée une heure libre tous les jours, mieux vaut l'utiliser de manière régulière pour vous permettre d'atteindre le but visé. Sans cela vous n'allez pas pouvoir atteindre le but que vous vous êtes fixé dès le départ. Il faut en plus de la passion, la discipline qui est très importante pour évoluer et, comme la définition l'a notifiée, c'est une imposition à se faire pour avancer dans le domaine de la sécurité. Cela doit être une obligation pour vous, et oui,

c'est une obligation imposée. Cela va vous permettre d'atteindre le sommet et le niveau d'expertise visé.

La passion et la discipline ne servent à rien si vous n'avez pas de bon formateur et de bons cours dans le domaine choisi.

D. Quatrième principe: Avoir des cours pragmatiques

Ce Point est très sensible surtout en Afrique où la sécurité informatique est apprise généralement de manière théorique, sans preuve, sans test valable et sans pratique dans des cas réels. Sachez tout simplement que si vos cours sont de la théorie votre niveau ne sera que médiocre malgré les principes 1,2 et 3.

Qu'est-ce que la pratique et quelles sont ses conséquences ?

La pratique : qui s'applique aux situations **concrètes**, qui maîtrise une technique, faculté à résoudre habilement les petits soucis de la vie quotidienne

Application des règles et des principes d'un art, d'une science ou d'une Technique.

La pratique est alors un levier très important en hacking et en sécurité informatique, un Hacker qui apprend la sécurité informatique sans la pratique réelle de ce qu'il fait n'est qu'un hacker de nom. Le hacking même est par définition une pratique, et non une théorie.

L'une des choses dans votre formation dans le hacking à exiger est la pratique, si non sans cela vous serez « nul » dans votre domaine malgré vos diplômes.

L'une des écoles qui privilégient « la pratique » que je vous conseille est :

www.gsimel.com

E. Cinquième principe : Avoir un mentor

Un mentor est une perle dans la sécurité informatique. Quel que soit ton niveau, tu dois obligatoirement avoir un mentor de près ou de loin car la sécurité en informatique est un domaine où pour avoir accès facilement à certaines choses comme les outils, il faut des personnes qui sont assez avancées en informatique. Les caractéristiques d'un bon mentor dans ce domaine sont: (1) c'est une personne qui est pragmatique et non théorique. (2) C'est une personne qui travaille durement, « qui bosse » toujours malgré son niveau. Sachez que l'informatique avance rapidement et on ne peut être à la tête que lorsque nous travaillons encore et encore pour être à jours dans « le système ».

(3) C'est une personne qui est ouverte ; si votre mentor n'est pas ouvert vous risquez d'évoluer lentement.

Si ces trois critères caractérisent votre mentor alors bonne chance à vous.

En résumé chaque principe est très utile pour atteindre le niveau d'expertise, et vous ne devez négliger aucun d'eux car ils sont importants surtout dans le domaine de la sécurité informatique.

Au reste, il reste une loi unique en son genre que vous ne devez pas laisser et c'est la plus grande de toutes : c'est principalement elle qui dirige tout :

La loi ultime

III/ La loi ultime

La loi ultime est « **Le travail** ». Si vous faites tout ce qui est recommandé dans « les principes » sans faire beaucoup de recherche et d'étude, vous ne serez rien. En vrai vous ne serez pas des experts avancés car ce que ce domaine exige dans chaque expertise est le travail. En français familier, nous parlons de « la bosse ».

Ce principe est le plus important.

NB : Recommandation: pour apprendre le Hacking des mobiles, Le hacking des entreprises, et pour leur sécurité rejoignez-nous sur www.gsimel.com, Vous aurez tout, du début à la fin.

Sans la Pratique avec un bon formateur l'échec est presque inévitable.

Merci à tous et à toutes et merci d'appliquer ces conseils d'expert pour avancer dans ce domaine.

MEL-ACADEMIE ET MEL-OUTILS (www.gsimel.com) sont à votre service.

IV/ Comment être un expert en sécurité système ?

1. Qu'est-ce qu'un système informatique ?

Un **système informatique** est un ensemble de moyens **informatiques** et de télécommunication ayant pour finalité d'élaborer, de traiter, de stocker, d'acheminer, de présenter ou de détruire des données.

Chaque entreprise dans le monde a besoin obligatoirement d'un expert en sécurité système. L'opportunité d'embauche est vraiment très élevée.

2. Qui est l'expert en sécurité système ?

Un expert en sécurité système est une personne capable de protéger les systèmes d'une entreprise ; plus particulièrement dans un réseau active directory (réseau d'entreprise créer par serveur).

3. Quelles sont les compétences d'un expert en sécurité système ?

- L'une des premières compétences d'un expert est le **piratage « Le hacking »**.
Pour devenir expert il faut obligatoirement avoir des bases en pénétration système de base, c'est-à-dire « faire du hacking réel, de système d'exploitation, faire de RDP, faire des vols de données d'un système, passer en administrateur sur un système, faire des captures des Caméras et autres

(...). Ceci est appris dans le cours 1 (Hacking base professionnel) de la MEL-ACADEMIE 100% Pratique www.gsimel.com.

•

- Un expert en sécurité système en devenir doit obligatoirement apprendre l'administration système serveur pour savoir comment les serveurs fonctionnent. Pourquoi ? simplement parce que tu ne peux pas faire une bonne sécurité d'entreprise si tu ne sais pas toi-même à la base comment fonctionne le système serveur d'une entreprise. Pour pallier à cela il y a le cours d'administration disponible sur www.gsimel.com.
- Un Hacker professionnel en « sécurité système » en devenir doit obligatoirement apprendre **le piratage** en entreprise, cela est très important car cela lui permet de découvrir le mode d'attaque des pirates afin de pouvoir donner des solutions à ces modes d'attaque. Cela lui permettra aussi d'être soi-même un bon hacker et aussi un bon penstester. Pour un cours de ce genre : « comment créer et pirater un réseau d'entreprise et comment pirater une entreprise sécurisée », allez sur www.gsimel.com
- Un Hacker doit également être un chercheur en vulnérabilité et doit savoir également comment l'espionnage se fait sur les systèmes pour éviter à l'entreprise des pertes de concurrence. Ceci est traité au début d'une rentrée académique de l'académie www.gsimel.com.
- La dernière des choses qu'un hacker doit apprendre c'est la sécurité des systèmes avancés en entreprise.

Avec ces compétences dévoilées, vous serez apte à travailler pour n'importe quelle entreprise sans craindre d'éventuelle attaque et si vous êtes déjà dans une entreprise, soyez vigilant, formez-vous car votre poste est menacé sans compétence réelle.

Du reste pour les autres domaines veuillez-vous faire vos propres recherches.

V/ Où trouver son inspiration ?

Pour avoir une inspiration il faut avoir un but et pour avoir un but il faut avoir une raison. La raison peut venir de votre de travail, d'une frustration, d'un film ou des demandes au niveau de la sécurité d'une ou plusieurs entreprises. Vous devez avoir une raison pour pouvoir être inspiré et l'une des pratiques pour avoir une raison facilement si vous n'en avez pas, c'est tout simplement d'en créer, par des films, des séries de hacking, ou être dans des sphères qui frustrant ou qui réveillent votre orgueil d'être toujours meilleur dans votre spécialité.

Avant d'avoir une inspiration il faut d'abord trouver une raison pour laquelle vous voulez devenir un expert dans un domaine précis en système de sécurité ou web, le reste viendra seul.

MERCI D'AVOIR LU CE COURS !

COMMENT DEVENIR UN EXPERT EN SECURITE INFORMATIQUE EN QUELQUES MOIS ?

Edition
mise à jour

**Maizan Kouame
Melchisedek**

Fonction : Président
directeur de Gsimel,
Testeur d'intrusion,
écrivain, consultant
informatique,
Formateur en sécurité
informatique.

Ce livre est un livre purement pédagogique et fait pour aider à construire une mentalité de hacker avancé afin d'avancer dans la sécurité de manière positive mais aussi pour ne pas prendre un mauvais chemin avec ce terrain où il y a beaucoup de tromperies et du mensonge de plusieurs instituts qui ne réalisent pas en réalité des performances pratiques donc qui n'arrivent pas à former en réalité.