Un membre du cours, Vincent Le Bouar, devenu récemment ***CEH*** (*Certified Ethical Hacker*) m'a accordé quelques minutes de son précieux temps pour partager son expérience avec vous.

Je lui ai posé une dizaine de questions qui pourraient vous intéresser si vous souhaitez vous aussi vous certifier et/ou si vous souhaitez progresser en sécurité informatique de manière générale.

﻿[](https://coachtestprep.s3.amazonaws.com/direct-uploads/user-15946/3755ed41-0da4-44ce-a57f-003e15fabf1d/CEH_2E345519D3F7.png)﻿

Voici l'interview :

**1. Tout d'abord, quel est votre parcours professionnel ?**

 J'ai une formation d'ingénieur Travaux Publics, donc pas vraiment dans le domaine de l'Informatique, même si nous faisions un peu de programmation (en Pascal), essentiellement pour faire de la modélisation. J'ai exercé pendant une vingtaine d'années dans le secteur public, j'étais en charge de la gestion d'un réseau routier.

Puis j'ai souhaité opérer une reconversion professionnelle. J'ai passé une licence professionnelle en droit pour pouvoir exercer comme enquêteur / détective privé. Je tiens à préciser que cette profession (autrefois sulfureuse) est aujourd'hui réglementée et contrôlée régulièrement. Nous ne pouvons intervenir que sur des missions dites "légitimes", ce qui signifie qu'il doit toujours y avoir un cadre et un fondement juridique. Pour ma part, je réalise beaucoup d'enquêtes d'assurances.

Souhaitant me spécialiser dans l'investigation numérique, j'ai décidé de passer la certification CEH, délivrée par l'EC Council, que je viens de réussir.

Je vais préparer dans la foulée la certification Computer Hacking Forensic Investigator (CHFI), afin de faire le lien avec le métier de l'enquête.

**2. Quel est le plan d'apprentissage que vous recommanderiez à un débutant désireux d'apprendre la sécurité informatique à partir de zéro ?**

Je ne sais pas si on peut apprendre réellement la sécurité informatique en tant que telle en partant de zéro.

Je pense qu'il est nécessaire de d'abord comprendre le fonctionnement des machines et des réseaux. Pour ma part, ce domaine m'a toujours passionné (fasciné ?), quitte à faire parfois (trop souvent sans doute) des expériences malencontreuses en manipulant la base de registre, les paramètres de la box, etc ...

Je pense donc qu'une bonne connaissance préalable des OS et du fonctionnement des réseaux est nécessaire.

Pour ma part, outre le blog du Hacker, j'ai trouvé des formations très intéressantes sur des sites comme Openclassrooms (voir le cours d'E. Lalitte sur les réseaux TCP/IP) ou bien développez.com. Il y a aussi FrameIP.com.

**3. Quels sont les points les plus difficiles à gérer ou à comprendre dans ce domaine ?**

Personnellement, lorsque j'ai suivi la formation CEH, j'ai eu des difficultés avec les modules Énumération (j'avais peu de connaissance sur l'Active Directory par exemple) et sur les failles Web (en particulier la Cross Site Request Forgery) ou Session Hijacking.

Je pense que ces domaines sont un peu plus difficile à appréhender pour un particulier car on n'a pas forcément les outils pour faire des tests chez soi, même si on trouve des machines vulnérables comme DVWA. Alors que pour le fonctionnement des réseaux, on peut toujours faire des essais avec des outils comme Wireshark pour écouter son propre trafic.

Quant au Buffer Overflow, ouh là !

**4. Quelles sont les compétences et les connaissances TECHNIQUES indispensables pour réussir ?**

Je répondrai à cette question par rapport à l'examen CEH, car cela permet de constituer un cadre assez formalisé.

Donc pour réussir cet examen, et avant de démarrer le cursus de formation, il est indispensable, je pense, de passer du temps sur le fonctionnement des réseaux TCP/IP et du modèle OSI. Ces notions reviennent tout le temps, tout au long des modules : scanning, sniffing, DOS, IDS, Firewall, Wireless, IoT.

Il faut avoir bien compris les principes de l’encapsulation des données, de l'authentification des machines, à quoi correspondent les couches du modèle, etc ...

**5. Quelles sont les qualités NON TECHNIQUES recommandées ?**

Je pense qu'il faut de la patience et de la persévérance, comme pour tout apprentissage finalement.

Il faut aussi de la méthode, car la sécurité informatique c'est très vaste. il y a toujours un risque de se disperser, surtout lorsque l'on apprend seul.

Enfin, il faut pratiquer, quitte à faire des erreurs (ou des fausses manipulations) d'ailleurs. Le travail nécessaire pour réparer ses erreurs n'est jamais du temps perdu.

Je précise que j'ai suivi la formation en e-learning : cela permet de se donner du temps pour approfondir des domaines si besoin. Clairement, j'aurais été incapable de suivre cette formation en présentiel ! Ceci dit, le temps passe vite, les manuels remis par EC Council représentent quand même 2500 pages en anglais. Je conseillerai de prendre le temps de les étudier, car les vidéos survolent parfois certains aspects.

**6. Quel a été la plus grosse surprise ou découverte lors de votre apprentissage ?**

Globalement, j'ai été surpris de découvrir la variété des vulnérabilités, même si la plus grosse vulnérabilité est sans doute la couche 8 du modèle OSI : l'être humain !

J'ai aussi compris qu'il n'existe pas de sécurité à 100%. En revanche, je n'irais pas jusqu'à dire qu'un pirate peut facilement faire ce qu'il veut. On peut quand même lui rendre la tâche difficile.

Si on prend l'exemple des mots de passe, il faut savoir que ceux-ci sont normalement chiffrés par un algorithme de hachage irréversible. Concrètement, on ne peut deviner le mot de passe qu'en faisant des essais. Si le mot de passe ne figure pas dans un dictionnaire, ne comporte pas d'informations personnelles (type le prénom suivi de la date de naissance), s'il est long, etc ... un craquage par brute force peut prendre quelques milliards d'années.

À noter que j'ai été agréablement surpris par la qualité des Labs proposés. On a accès à plusieurs machines virtuelles, et ça fonctionne très bien (bien mieux qu'à la maison avec Virtualbox ou similaire !).

**7. Quel est selon vous l'avantage de suivre en amont des cours vidéo sur le Hacking éthique ?**

En fait, tout est bon pour apprendre, les cours vidéos comme les livres ou les sites écrits.

Les vidéos sont plus vivantes, on peut faire les manipulations en même temps. En revanche, lorsque l'on souhaite rechercher un point précis (comme la syntaxe d'une ligne de commande, parce qu'on l'a mal notée), ça peut être compliqué. Il faut utiliser plusieurs supports.

**8. Comment mettre toutes les chances de son côté pour passer avec succès la certification CEH ?**

Au risque de décevoir, pour réussir l'examen, il faut quand même bachoter aussi !

Et il faut se placer dans une logique d'examen, car il y a des points qui sont faciles à prendre. Je sais bien que cela peut choquer, mais si on décide de passer un examen, autant jouer le jeu : ce serait un peu idiot d'être techniquement hyper compétent et d'échouer à cause de questions dont on ne comprend pas vraiment l'intérêt.

Il y a un pool de questions sur tous les sujets. Pour l'examen, les questions sont tirées au sort pour chacun des candidats. Je pense malgré tout que la plupart des domaines concernés sont représentés suivant une certaine proportion. Il y aura forcément des question pas du tout techniques dans le lot.

Par exemple, il peut y avoir des questions sur la réglementation US ! Clairement, pas beaucoup d'intérêt. D'un autre côté, il y a peine 10 lois à connaître, donc c'est faisable. Il peut y avoir aussi une ou deux questions sur les n°s de ports (en général, ce sont des n°s assez courants).

**9. Qu'est-ce que la certification CEH vous permet dorénavant de faire et de démontrer ?**

Le principe de la certification permet finalement de reconnaître une certaine compétence de la personne, alors qu'on n'a pas forcément un diplôme dans ce domaine. Ce n'est évidemment pas reconnu par l'Éducation Nationale, mais ça l'est par la NSA, donc ...

Ceci étant, je me considère tout au plus comme un bidouilleur, et je n'ai absolument pas la prétention de me comparer à un authentique informaticien. De toute façon, on trouve toujours meilleur que soi.

Sinon, la CEH est un peu la pierre angulaire des cursus de formation. Lorsque l'on a réussi la CEH, on peut s'orienter ensuite vers le test d'intrusion (Licence Penetration Tester) ou l'investigation (CHFI).

Pour moi, c'était donc surtout une étape pour aller vers la CHFI.

Un grand merci à Vincent pour ses réponses et pour sa participation. Vous pouvez le rejoindre sur LinkedIn : <https://www.linkedin.com/in/vincent-le-bouar-75a171131/>