

Lead Ethical Hacker



1. Présentation

Quotidiennement, les organisations comme les personnes utilisent de nombreux systèmes, de réseaux ou encore d'applications informatiques pour répondre à de multiples besoins. Ces nombreux environnements informatiques peuvent comporter d'importantes vulnérabilités et sont exploitées à travers des actes malveillants.

Améliorer la sécurité globale des organisations est maintenant devenu un impératif. Cela demande de combler les écarts et les vulnérabilités identifiés lors de tests d'intrusion par un pirate éthique. Les pirates éthiques sont autorisés à utiliser les mêmes techniques de piratage que les pirates malveillants.

Les pirates éthiques sont également connus sous le nom de « white hats hackers », ils utilisent leur expertise en matière de piratage pour améliorer la sécurité des organisations en réduisant le nombre de vulnérabilités et de violations de la sécurité.

A travers une session de cinq (5) jours, les participant(e)s pourront développer les compétences nécessaires pour effectuer du piratage éthique, principalement pour les tests d'intrusion des systèmes d'information et des réseaux. Au-delà de l'approche théorique, le cours comprend également des laboratoires qui sont réalisés avec une machine virtuelle.

2. Objectifs

- Maîtriser les concepts, méthodes et techniques utilisés par les organisations de cybersécurité et les hackers éthiques pour réaliser des tests d'intrusion ;
- Reconnaître la corrélation entre les méthodologies de tests d'intrusion et d'autres standards internationaux ;
- Acquérir une connaissance approfondie des composantes et opérations du piratage éthique.

3. Public cible

Cette formation s'adresse principalement aux professionnels impliqués dans la sécurité de l'information, nous pouvons citer parmi eux : responsables de la sécurité de l'information, acteurs en charge du piratage éthique et de tests d'intrusion, praticiens de la sécurité de l'information, consultants en sécurité de l'information.

4. Durée

05 jours

5. Prérequis

Il est recommandé que les participant(e)s disposent d'une connaissance des concepts et principes de sécurité de l'information et de compétences avancées en matière de systèmes d'exploitation.

6. Certification

L'examen -PECB Certified Lead Ethical Hacker- est inclus dans le coût de la formation et est disponible en langue française.

L'examen a une durée de six (6) heures et couvre les six domaines suivants :

Domaine 1 : Outils et techniques de collecte d'informations

Domaine 2 : Modélisation des menaces et identification des vulnérabilités

Domaine 3 : Techniques d'exploitation

Domaine 4 : Escalade des droits

Domaine 5 : Pivotement et transferts de fichiers

Domaine 6 : Rapports

Il est à noter que l'examen est composé de deux parties : l'examen pratique et la rédaction du rapport. L'examen pratique exige du candidat qu'au moins deux machines soient compromises au moyen des tests d'intrusion. Le processus doit être documenté dans un rapport écrit.

7 Programme

- Jour 1** Introduction au piratage éthique
- Jour 2** Lancement de la phase de reconnaissance
- Jour 3** Lancement de la phase d'exploitation

- Jour 4** Post-exploitation et rapports
- Jour 5** Préparation à l'examen et examen de certification