Réaliser des tests d’intrusion (Sécurité Pentesting) avec CLEH - CEH

Date et durée

Code formation : SP-RS6092
Durée : 4,5 jours
Nombre d'heures : 31 heures

Description

La certification « Réaliser des tests d'intrusion (Sécurité Pentesting) » s'adresse aux professionnels de la sécurité informatique et permet d'acquérir toutes les compétences indispensables pour effectuer des tests qui consistent à examiner tous les réseaux et les systèmes informatiques en simulant les actions d'un intrus potentiel à l'intérieur de leur environnement de travail : analyse des flux, analyse des espaces de stockages, analyse de sécurité spécifique au terminal utilisé. En outre, cette formation est compatible avec le programme CLEH - CEH, offrant ainsi une dimension supplémentaire à votre expertise en sécurité pentesting.
En suivant cette formation, vous acquerrez les compétences et les connaissances nécessaires pour maîtriser les différentes phases d'une attaque, identifier les types de menaces, mettre en œuvre des contre-mesures efficaces, et exécuter des tests pratiques sur des scénarios réels. Les travaux pratiques intensifs, combinés à des exercices d'évaluation, vous permettront de développer une compréhension approfondie de la sécurité pentesting. Vous serez ainsi prêt à appliquer ces compétences sur le terrain, renforçant non seulement votre expertise, mais également votre capacité à anticiper et à contrer les cybermenaces.
Que vous soyez un professionnel de la sécurité informatique débutant ou un technicien, cette formation est indispensable pour toute entreprise qui souhaite protéger ses actifs numériques, répondre aux exigences et garder une longueur d’avance sur l’évolution des cybermenaces.

M2I Formation est un organisme qui délivre des formations dans les secteurs de l'informatique, du digital et de la cybersécurité.

Objectifs

A l’issue de cette formation, vous atteindrez les objectifs suivants :

- Comprendre les principes de base de la sécurité informatique;
- Identifier les menaces et les risques;
- Utiliser les outils et les techniques de sécurité informatique;
- Définir les enjeux et contraintes du test d’intrusion dans l’objectif de définir les scénarios les plus probables ainsi que l’obtention du consentement légal;
- Appliquer une méthodologie de test d’intrusion claire et reproductible afin de pouvoir restituer des éléments comparables dans leurs approches;

- Concevoir et réaligner des outils d’intrusion dans l’objectif de répondre aux différents besoins d’un test d’intrusion;
- Identifier les différentes vulnérabilités présentes en réalisant les différentes phases des tests d’intrusion évoqués dans les enjeux initiaux dans le but de découvrir les points de faiblesses de l’organisation;
- Remonter et restituer les différentes vulnérabilités identifiées ainsi qu’un plan d’actions contenant les mesures de sécurité permettant à l’organisation de corriger ses failles;

Points forts

Une formation certifiante en sécurité informatique est accessible à tous les professionnels du secteur, des cours accompagnés d'exercices d'évaluation (QCM) et une mise en situation professionnelle.

Certification

Cette formation permet d'obtenir la certification « **Réaliser des tests d'intrusion (Sécurité Pentesting)** », enregistrée par France Compétences sous le numéro RS6092. Destinée aux professionnels de la sécurité informatique, elle prouve que vous êtes capable de réaliser des tests d'intrusion.
L'examen de certification d'une durée de 4h consiste en une mise en situation professionnelle à partir d'un besoin exprimé ou généré.

1. Réalisation d'un mini projet dans le cadre d'une étude de cas
2. Mise en situation professionnelle : Sélectionner les outils et exploiter les différentes vulnérabilités pour effectuer un test d'intrusion

Le candidat présentera un rapport au jury qu’il défendra à l’oral durant un temps maximum de 1H30 en détaillant la méthode, les outils choisis ainsi que les contre mesure adéquates vis-à-vis des menaces et vulnérabilités identifiées lors de son penteste.
Une grille d’évaluation est complétée par le jury avec **un score minimal de 60/100 pour la validation de l’ensemble des compétences de la certification et réparti comme suit:**

- **60%** pour l’épreuve certificative
- **40%** pour la soutenance

Modalités d'évaluation

Quiz / QCM
Travaux Pratiques

Pré-requis

Suivre cette formation nécessite les prérequis suivants :

- Avoir des connaissances de base en réseaux : protocoles, adressage IP, routage ...
- Avoir une compréhension du fonctionnement des systèmes Linux et/ou Windows : commandes de base, systèmes de fichiers
- Être familier avec les systèmes de virtualisation comme VMWare, Hyper-V ou virtual Box
- Avoir une appétence pour les grands domaines de la cybersécurité : sécurité des systèmes, des réseaux, des applications

Public

Cette formation s'adresse aux publics suivants :

- Techniciens systèmes et réseaux
- Administrateurs systèmes et réseaux

- Développeurs ayant une bonne connaissance des systèmes et réseaux
- Analystes SOC
- Professionnels de la cybersécurité souhaitant évoluer vers le pentest.

Cette formation s'adresse aux profils suivants

Pentester (tests d'intrusion)
Administrateur système
Ingénieur système
Responsable sécurité informatique
Analyste cybersécurité
Directeur des Systèmes d'Information (DSI)

Programme

Tour de table

- Introduction individuelle
- Exploration des attentes et des objectifs de chaque participant
- Introduction au cadre de la formation
- Alignement avec les objectifs et enjeux spécifiques
- Identification des attentes et des perspectives individuelles des participants
- Information sur l'organisation des épreuves de certification
- Inscription de chaque participant aux épreuves de certifiation

---

Jour 1: Fondamentaux de la sécurité et terminologie

- Introduction à la sécurité de l'information
- Terminologie et culture générale du pentesting
    - Le jargon du pentester
    - Les hacks et les hackers célèbres
    - La virtualisation
- Sécurité des systèmes d’information
    - Vulnérabilités, menaces, risques, véracité, gravité
- Les 5 phases d’une attaque
    - La reconnaissance
    - Le scan de vulnérabilités
    - L'obtention de l'accès
    - Le maintien de l’accès
    - L'effacement des traces
- *Exercice d'évaluation: QCM*

Jour 2: Menaces et contre-mesures

- Malwares
    - Trojan, backdoor, virus, ver informatique
- Attaques de déni de service
    - DoS, DDoS, DrDoS
- Ingénierie sociale
    - Phishing, spearphishing, Google Dorks
- Cryptographie
    - Chiffrement symétrique, chiffrement asymétrique, certificats de chiffrement

- *Exercice d'évaluation: QCM*

Jour 3: Types d'attaques

- Attaques des réseaux
    - Réseaux sans fils (WiFi), réseaux filaires, spoofing
- Attaques des systèmes
    - Emprunt d'identité, vol de session, escalade de privilèges
- Attaques des serveurs web
    - Concept de serveur web, contremesures, méthodologie des attaques
- Attaques des applications Web
    - Concept d’application Web, API Web, WebHooks, Web shell, méthodologie des attaques
- *Exercice d'évaluation: QCM*

Jour 4: Processus d'une attaque

- Reconnaissance
    - Outils de reconnaissance
- Prise d’empreinte
    - Scan
- Enumération
    - Scan approfondi
- L’analyse
- *Exercice d'évaluation: QCM*

Jour 5: Travaux pratiques et applications

- Travaux pratiques
    - Détecter les failles de sécurité
    - Rédaction d'un rapport
    - Utilisation d'une machine virtuelle sous Linux
    - 4 heures d'exercices pratiques
- Application des compétences acquises sur des scénarios réels