Programme de cours
ETHICAL HACKING

Durée :	5 jours soit 35 heures	Référence :	SEC5

Public visé :

- Consultants en sécurité
- Techniciens
- Administrateurs systèmes/réseaux

Pré-requis :

- Bonnes connaissances en sécurité SI, réseaux, systèmes (en particulier Linux) et en programmation

Objectifs pédagogiques :

- Comprendre les techniques des pirates informatiques et pouvoir contrer leurs attaques
- Mesurer le niveau de sécurité de votre Système d'Information
- Réaliser un test de pénétration
- Définir l'impact et la portée d'une vulnérabilité

Modalités pédagogiques :

Session dispensée en présentiel ou téléprésentiel, selon la modalité inter-entreprises ou intra-entreprises sur mesure.
La formation est animée par un(e) formateur(trice) durant toute la durée de la session et présentant une suite de modules théoriques clôturés par des ateliers pratiques validant l'acquisition des connaissances. Les ateliers peuvent être accompagnés de Quizz.
L'animateur(trice) présente la partie théorique à l'aide de support de présentation, d'animation réalisée sur un environnement de démonstration.
En présentiel comme en téléprésentiel, l'animateur(trice) accompagne les participants durant la réalisation des ateliers.

Moyens et supports pédagogiques :

Cadre présentiel
Salles de formation équipées et accessibles aux personnes à mobilité réduite.
- Un poste de travail par participant
- Un support de cours numérique ou papier (au choix)
- Un bloc-notes + stylo
- Vidéoprojection sur tableau blanc
- Connexion Internet
- Accès extranet pour partage de documents et émargement électronique

Cadre téléprésentiel
Session dispensée via notre solution iClassroom s'appuyant sur Microsoft Teams.
- Un compte Office 365 par participant
- Un poste virtuel par participant
- Un support numérique (PDF ou Web)
- Accès extranet pour partage de documents et émargement électronique

Modalités d'évaluation et suivi :

Avant
Afin de valider le choix d'un programme de formation, une évaluation des prérequis est réalisée à l'aide d'un questionnaire en ligne ou lors d'un échange avec le formateur(trice) qui validera la base de connaissances nécessaires.
Pendant
Après chaque module théorique, un ou des ateliers pratiques permettent la validation de l'acquisition des connaissances. Un Quizz peut accompagner l'atelier pratique.
Après
Un examen de certification si le programme de formation le prévoit dans les conditions de l'éditeur ou du centre de test (TOSA, Pearson Vue, ENI, PeopleCert)
Enfin
Un questionnaire de satisfaction permet au participant d'évaluer la qualité de la prestation.

Description / Contenu

Module 1 : Le monde du hacking
- Introduction
- Pratique et mémétiques
- Déclinaisons commerciales

Module 2 : La vie d'une vulnérabilité
- Acteurs et Autorité
- Que faire d'une vulnérabilité
- Responsible disclosure
- Métrique et évaluation de l'impact

Module 3 : Technique de reconnaissance et nom de domaine
- Les ressources sources ouvertes
- Le service DNS
- Fuites d'informations

Module 4 : Comprendre le scan et énumération
- Scan réseaux
- Scan de vulnérabilités

Module 5 : Automatiser la collecte
- Red team vs Blue team

- Red team Automation
- Continuous pentesting

Module 6 : Structure d'un monde Web

- Introduction
- Anatomie du protocole HTTP
- La modernisation de la technologie (Protection navigateurs, ressources externes...)

Module 7 : Introduction à l'OWASP top 10

- Présentation de l'OWASP
- Analyse de l'OWASP top 10
- Études et mise en application

Module 8 : Rappel sur la structure d'un système

- Rappel sur le rôle des composants
- Rappel sur les systèmes d'exploitation
- Introductions aux mécanismes de protection

Module 9 : Exploitation de buffer overflow

- Introduction à l'exploitation applicative
- Rappel sur l'exécution d'une application
- Exploitation d'un buffer overflow

Module 10 : Les méthodes de détection modernes

- Le SOC gardien du SI
- EDR/XDR
- Threat intel

Module 11 : Contournement et post-exploitation

- Introduction à la « psych-war »
- Présentation de méthode de contournement de détection
- Metasploit un framework d'exploitation.