HACKING ET SÉCURITÉ PERFECTIONNEMENT

Public	Consultants en sécurité Ingénieurs / Techniciens Administrateurs systèmes / réseaux Développeurs
Durée	5 jours - 35 heures
Pré-requis	Connaissances de TCP/IP La maîtrise de Linux en ligne de commande est un plus
Objectifs	Comprendre comment organiser une veille sur la sécurité et savoir où rechercher des informations fiables Identifier les "faiblesses" des éléments constitutifs du SI par des prises d'empreintes Disposer des compétences techniques nécessaires pour réaliser différentes attaques et ainsi en comprendre les subtilités Être en mesure de protéger le SI par un système de contre-mesures adaptées
Méthodes pédagogiques	Pour bien préparer la formation, le stagiaire remplit une évaluation de positionnement et fixe ses objectifs à travers un questionnaire. La formation est délivrée en présentiel ou distanciel (e-learning, classe virtuelle, présentiel et à distance). Le formateur alterne entre méthodes démonstratives, interrogatives et actives (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification. Cette formation est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par Audit Conseil Formation.
Moyens techniques	1 poste de travail complet par personne De nombreux exercices d'application Mise en place d'ateliers pratiques Remise d'un support de cours Passage de certification(s) dans le cadre du CPF Remise d'une attestation de stage
Modalité d'évaluation des acquis	Evaluation des besoins et objectifs en pré et post formation Evaluation technique des connaissances en pré et post formation Evaluation générale du stage
Délai d'accès	L'inscription à cette formation est possible jusqu'à 5 jours ouvrés avant le début de la session
Accessibilité handicapés	Au centre d'affaires ELITE partenaire d'ACF à 20 m. Guide d'accessibilité à l'accueil.

INTRODUCTION

- Rappels sur TCP/IP

INTRODUCTION À LA VEILLE

- Vocabulaire
- Base de données de vulnérabilité et exploitation
- Informations générales

PRISE D'INFORMATIONS

- Informations publiques
- Moteur de recherches
- Prise d'information active

SCAN ET PRISE D'EMPREINTE

- Énumération des machines
- Scan de ports
- Prise d'empreinte du système d'exploitation
- Prise d'empreinte des services

VULNÉRABILITÉS INFORMATIQUES

- Vulnérabilités réseau
- Vulnérabilités applicatives
- Vulnérabilités web
- Exploitation des vulnérabilités
- Maintien de l'accès à une machine

ATELIER PRATIQUE EN LABORATOIRE

- Mise en oeuvre d'une stratégie d'attaque sur un laboratoire créé spécialement pour la formation
- Lancement de l'attaque et tentative d'exploitation
- Capture de drapeau
- Étude des contre-mesures appropriées

NOUS CONTACTER

Siège social
16, ALLÉE FRANÇOIS VILLON
38130 ÉCHIROLLES

Téléphone
04 76 23 20 50 - 06 81 73 19 35

Suivez-nous sur les réseaux sociaux, rejoignez la communauté !

ACF Audit Conseil Formation

@ACF_Formation

Dernière mise à jour : 27/09/2023

PROFIL Formateur : Les formateurs sont recrutés selon plusieurs critères :
Expérience, pédagogie, dynamisme et prévoyance.