HACKING ET SECURITE LES FONDAMENTAUX

Public	Consultants en sécurité Ingénieurs / Techniciens Administrateurs systèmes / réseaux Toute personne intéressée par la pratique de la sécurité
Durée	4 jours - 28 heures
Pré-requis	Connaissances de base de Windows ou Linux
Objectifs	Comprendre comment il est possible de s'introduire frauduleusement sur un système distant Savoir quels sont les mécanismes en jeu dans le cas d'attaques système Acquérir les compétences nécessaires pour mettre en place un dispositif global garantissant la sécurité des systèmes
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 démonstrative, interrogative et active (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.

1. INTRODUCTION SUR LES RÉSEAUX

- Prise d'informations (Prise d'informations à distance sur des réseaux d'entreprise et des systèmes distants)
- Informations publiques
- Localiser le système cible
- Énumération des services actifs

2. ATTAQUES À DISTANCE

- Intrusion à distance des postes clients par exploitation des vulnérabilités sur les services distants, et prise de contrôle des postes utilisateurs par troyen
- Authentification par brute force
- Recherche et exploitation de vulnérabilités
- Prise de contrôle à distance

3. ATTAQUES SYSTÈMES

- Attaques du système pour outrepasser l'authentification et/ou surveiller l'utilisateur suite à une intrusion
- Attaque du Bios
- Attaque en local
- Cracking de mot de passe
- Espionnage du système

4. SÉCURISER LE SYSTÈME

- Outils de base permettant d'assurer le minimum de sécurité à son S.I.
- Cryptographie
- Chiffrement des données
- Détection d'activité anormale
- Initiation à la base de registre
- Firewalling
- Anonymat

NOUS CONTACTER

Siège social
16, ALLÉE FRANÇOIS VILLON
38130 ÉCHIROLLES

Centre de formation
87, RUE GÉNÉRAL MANGIN
38000 GRENOBLE

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

E-mail
contact@audit-conseil-formation.com

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

ACF Audit Conseil Formation @ACF_Formation ACFauditconseilformation