COMPROMISSION ET SÉCURISATION DE L'ACTIVE DIRECTORY

Public	Administrateurs Windows, support informatique, RSSI, pentesteurs.
Durée	4 jours - 28 heures
Pré-requis	Connaissances de base sur Windows, l'Active Directory, les réseaux et la sécurité informatique.
Objectifs	Décrire les mécanismes internes Active Directory Identifier les fonctionnalités de sécurité Concevoir une architecture robuste Connaître et mettre en œuvre les attaques et principales exploitations d'un réseau Active Directory Mettre en œuvre les contre-mesures Reconstruire son Active Directory en cas de compromission
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.

1. LES FONDAMENTAUX EN SÉCURITÉ DE L'ACTIVE DIRECTORY

- Comprendre une architecture Active Directory typique.
- Comprendre la méthodologie de compromission d'un Active Directory.
- Les principaux vecteurs d'attaques utilisés pour la compromission de l'Active Directory.
- Revue de l'authentification/autorisation.
- Tour d'horizon des différents protocoles.
- Comprendre les recommandations et bonnes pratiques associées.

2. COMPRENDRE LES RISQUES ET LES ATTAQUES

- Vue d'ensemble des méthodes de gestion des risques SI.
- Méthodologie de compromission d'un Active Directory (on-premise).
- Comprendre les différentes étapes d'une attaque.
- Simuler des attaques et analyser les contre-mesures.
- Détecter les failles de sécurité.
- Vue d'ensemble des outils associés.

3. DURCISSEMENT DE L'INFRASTRUCTURE AD

- Concevoir un plan de durcissement.
- Déployer les directives associées.
- Auditer une infrastructure.
- Collecter les événements au niveau de l'entreprise.
- Mettre en œuvre les directives préconisées et les nouveautés de durcissement (PAM, JIT/JEA...).

4. GÉRER UNE COMPROMISSION DE SON ACTIVE DIRECTORY

- Les grandes étapes de la gestion d'incident de l'AD.
- La gestion et la communication de crise.
- La reconstruction de l'AD.

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