EduGroupe
Accompagner pour réussir

Compromission et sécurisation de l'Active Directory

Référence : **SECAD** Durée : **4 jours (28 heures)** Certification : **Aucune**

Connaissances préalables

- Connaissances de base sur Windows, l'Active Directory, les réseaux et la sécurité informatique

Profil des stagiaires

- Administrateurs Windows, support informatique, RSSI, pentesteurs

Objectifs

- À l'issue de la formation, le participant sera en mesure de :
- 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

Certification préparée

- Aucune

Méthodes pédagogiques

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques et de réflexions
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

Formateur

- Consultant-formateur expert de l'Active Directory

Méthodes d'évaluation des acquis

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

EduGroupe
Accompagner pour réussir

Contenu du cours

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
- 💡 *Travaux pratiques tutorés*

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
- 💡 *Travaux pratiques : Mettre en œuvre les attaques et principales exploitations d'un réseau Active Directory*

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…)
- 💡 *Travaux pratiques tutorés : Mettre en oeuvre le durcissement de l'infrastructure AD*

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
- 💡 *Travaux pratiques : Mettre en œuvre les contre-mesures*

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.