Compromission et sécurisation de l'Active Directory

Cours Pratique de 4 jours - 28h
Réf : ADK - Prix 2024 : 2 790€ HT

Lors de cette formation, vous verrez quelles méthodologies et techniques sont utilisées par les attaquants, de l'accès anonyme jusqu'à la compromission totale de l'environnement. Vous apprendrez comment sécuriser son Active Directory (AD) et gérer une situation de crise après compromission de tout son réseau.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant 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

MÉTHODES PÉDAGOGIQUES

Méthode expositive, démonstrative et active.
Alternance entre présentation, démonstration et mise en pratique.

PARTICIPANTS

Administrateurs Windows, support informatique, RSSI, pentesteurs.

PRÉREQUIS

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

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

LE PROGRAMME

dernière mise à jour : 02/2024

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.

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.

LES DATES

CLASSE À DISTANCE
2024 : 23 sept., 12 nov.

PARIS
2024 : 16 sept., 05 nov.