Date de publication : 20/01/2025

Formation : Sécurité offensive de l'Active Directory, niveau 1

Formation pratique - 4j - 28h00 - Réf. SDB
Prix : 2410 € H.T.

Cette formation vous apprendra les techniques indispensables pour mesurer le niveau de sécurité de votre Active Directory. A la suite de ces attaques, vous acquerrez les compétences nécessaires à la réalisation d'un test d'intrusion Active Directory, la méthodologie et les techniques utilisées lors d'une intrusion.

Objectifs pédagogiques

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

- Comprendre l'architecture et les principes de fonctionnement d'Active Directory (AD)
- Maîtriser les techniques d'attaque et d'analyse d'un environnement AD
- Identifier les vulnérabilités courantes et y remédier
- Mettre en place des mesures préventives pour sécuriser les infrastructures AD

Public concerné

Pentesters, administrateurs système et responsables sécurité et professionnels en cybersécurité.

Prérequis

Bonne connaissance des environnements Windows et des concepts réseau.

Vérifiez que vous avez les prérequis nécessaires pour profiter pleinement de cette formation en faisant ce test.

Méthodes et moyens pédagogiques

Travaux pratiques

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

PARTICIPANTS

Pentesters, administrateurs système et responsables sécurité et professionnels en cybersécurité.

PRÉREQUIS

Bonne connaissance des environnements Windows et des concepts réseau.

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.

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.

Programme de la formation

1 Théories fondamentales et techniques d'attaque initiales

- Compréhension des mécanismes d'administration (RPC, SMB, WMI, etc.).
- Gestion des identités et des accès (NTLM, Kerberos).

2 Reconnaissance

- Techniques et outils d'OSINT (images, emails, identifiants, sites web, etc).
- Reconnaissance depuis un accès anonyme et un accès authentifié.
- Techniques avancées de reconnaissance et d'exploitation réseau.

3 Mouvements latéraux

- Empoisonnement ADIDNS, WinRM et JEA, extraction de secrets LAPS, gMSA/sMSA,
- Abus de liens de confiance MS-SQL, relaying NTLM, coercing d'authentification.
- Relai Kerberos, pivots inter-forêts, pivots vers Azure (PHS, PTA, ADFS), pivots depuis Azure (Intune).

4 Elévation de privilèges

- Elévation de privilèges locale : access token et impersonation, étude des vulnérabilités potatoes.
- Bypass des restrictions logicielles (AppLocker, environnements restreints comme Citrix).
- Elévation de privilèges sur le domaine : étude et abus des ACL, exploitation avancée de délégation Kerberos, ADCS, abus de groupes privilégiés.
- Analyse de vulnérabilités publiques, rejeu d'authentification, kerberoasting, abus de chemins de contrôle.

5 Extraction de secrets et techniques de persistance de l'Active Directory

- Extraction et manipulation de secrets critiques : LSASS, DPAPI, Kerberoasting.
- Persistance : ADCS (certificats), tickets Kerberos (golden, diamond, sapphire), DSRM, golden gMSA, abus AdminSDHolder.
- Création de skeleton key, délégation Kerberos, empoisonnement de GPO.
- Extension de la compromission : études des relations de confiance inter-domaines/inter-forêts.
- Abus de délégation Kerberos.

Dates et lieux

CLASSE À DISTANCE
2026 : 7 avr., 30 juin, 6 oct., 8 déc.

PARIS LA DÉFENSE
2026 : 23 juin, 29 sep., 1 déc.

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 formations pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
- À l'issue de chaque formation 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 participant 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

Pour toute question ou besoin relatif à l'accessibilité, vous pouvez joindre notre équipe PSH par e-mail à l'adresse psh-accueil@orsys.fr.