Date de publication : 20/01/2025

Formation : Sécurité offensive de l'Active Directory, niveau 2

Formation pratique - 4j - 28h00 - Réf. SDC
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 :

- Maîtriser les techniques avancées d'exploitation en environnement Active Directory
- Identifier et exploiter des configurations et vulnérabilités complexes
- Travailler sur des scénarios réalistes dans des environnements d'entreprise simulés

Public concerné

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

Prérequis

Bonne connaissance des environnements Windows et des concepts réseau. Ou connaissances équivalentes à celles apportées par le cours "Sécurité offensive de l'Active Directory, niveau 1" (réf. SDB).

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. Ou connaissances équivalentes à celles apportées par le cours "Sécurité offensive de l'Active Directory, niveau 1" (réf. SDB).

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

- Les techniques d'attaque initiales.
- Compréhension des mécanismes d'administration (RPC, SMB, WMI, etc.).

2 Techniques de contournement des équipements de sécurité

- Techniques de contournement des anti-virus.
- Techniques de contournement de l'AMSI.
- Techniques de contournement des EDRs.

3 Azure et à la compromission des environnements Azure

- Concepts fondamentaux d'Azure et intégration avec Active Directory.
- Techniques de reconnaissance et de compromission dans des environnements hybrides.

4 Active Directory et red-teaming

- Collecte d'informations pour une opération Red Team.
- Masquer ses attaques.
- L'outillage offensif pour la red team.
- Compromission d'équipements de type SCCM.

5 Développement d'outils offensifs

- Introduction au développement d'outils offensifs en C# sous Windows.
- Les principaux frameworks et bibliothèques C# utiles pour le développement d'outils offensifs (.NET, WinAPI, P/Invoke).
- Création de projets en C# pour le développement d'outils offensifs.
- Utilisation des outils de débogage pour la création et la maintenance des outils.
- Présentation des principaux services Active Directory (ex: DNS, LDAP, Kerberos, etc.).
- Attaques contre le protocole Kerberos dans Active Directory.
- Développement d'outils pour l'attaque et la défense de l'Active Directory.

Dates et lieux

CLASSE À DISTANCE
2026 : 23 juin, 29 sep., 1 déc.

PARIS LA DÉFENSE
2026 : 16 juin, 22 sep., 24 nov.

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.