New

Sécurité offensive de l'Active Directory

Analyse des alertes et orchestration de la réponse aux incidents

Présentiel ou en classe à distance

4 jours (28 h)

Prix inter : 3.150,00 € HT
Forfait intra : 7.490,00 € HT

Réf.: SR389

La formation **Sécurité offensive de l'Active Directory** propose une immersion complète dans les **techniques d'attaque avancées** ciblant les environnements **Microsoft Active Directory**. Conçue pour les pentesters, professionnels de la cybersécurité et administrateurs système, elle couvre l'ensemble du cycle d'une compromission : reconnaissance, mouvements latéraux, élévation de privilèges, extraction de secrets et persistance. Les participants approfondissent les mécanismes critiques de l'AD, notamment **Kerberos, NTLM, ACL, ADCS, GPO, LAPS, gMSA**, ainsi que les vecteurs d'attaque modernes comme **Kerberoasting, NTLM Relay, ADIDNS poisoning, exploitation des trusts inter-domaines** et scénarios hybrides on-prem / Azure.
Grâce à une approche résolument offensive et technique, la formation met l'accent sur la compréhension des failles d'architecture, l'abus des relations de confiance et l'exploitation des erreurs de configuration courantes. Les modules dédiés à l'élévation de privilèges, à l'extraction de credentials (LSASS, DPAPI) et aux mécanismes de persistance avancée (Golden Ticket, ADCS, AdminSDHolder, GPO poisoning) permettent aux participants de maîtriser les techniques utilisées lors d'attaques réelles.

A qui s'adresse cette formation ?

Pour qui

- Pentesters et professionnels en cybersécurité
- Administrateurs système et responsables sécurité

Prérequis

- Bonne connaissance des environnements Windows et des concepts réseau
- Disposez-vous des connaissances nécessaires pour suivre cette formation ? Testez-vous !

Programme

1 - Mécanismes fondamentaux d'administration et d'authentification

- Analyse des mécanismes d'administration distants : RPC, SMB, WMI, services exposés et vecteurs de risque
- Gestion des identités et des accès : fonctionnement interne de NTLM et Kerberos, dérivations clés, stratégies d'affaiblissement, usages détournés

2 - Reconnaissance (OSINT et activités sur le réseau)

- Techniques et outils OSINT : extraction d'informations depuis images, emails, identifiants, métadonnées, sites web, fuites diverses
- Reconnaissance depuis un accès anonyme : cartographie des services, découverte des endpoints, enumeration minimale
- Reconnaissance depuis un accès authentifié : expansion de la visibilité, collecte avancée d'informations AD, topologie réseau
- Exploration des techniques avancées de reconnaissance et d'exploitation réseau : scan passif/actif, découverte de services AD, analyse du trafic

3 - Techniques de pivot et d'abus des services AD

- Empoisonnement ADIDNS pour interception et redirection
- Abus de WinRM, exploitation des restrictions ou contournements JEA
- Extraction et exploitation des secrets LAPS, gMSA/sMSA

4 - Exploitation des relations et des protocoles

- Abus de liens de confiance MS-SQL pour exécution distante
- NTLM relaying et techniques modernes de coercition d'authentification
- Kerberos relay, limites et scénarios d'exploitation.

5 - Pivots inter-domaines / inter-forêts / cloud hybride

- Pivots inter-forêts AD : attaques sur trusts, délégations, SIDHistory
- Pivots vers Azure : exploitation PHS, PTA, ADFS
- Pivots depuis Azure : exploitation des configurations Intune, transition vers les ressources AD internes.

6 - Élévation locale Manipulation d'a

- Manipulation d'access tokens, mécanismes d'impersonation
- Analyse des vulnérabilités Potato et dérivés
- Contournement des restrictions logicielles : bypass AppLocker, environnements restreints (Citrix / RDS / shells limités)

7 - Élévation sur le domaine

- Étude et abus des ACL : Object ACL, DACL, ACE mal configurées
- Exploitation avancée de la délégation Kerberos (constrained, unconstrained, resource-based)
- Compromission et détournement de ADCS : attaques sur les templates, ESC1–ESC13
- Abus des groupes privilégiés, chemins d'accès privilégiés et erreurs d'architecture
- Exploitation des vulnérabilités publiques pertinentes via rejeu d'authentification, attaques Kerberoasting, manipulation des chemins de contrôle BloodHound

8 - Extraction et manipulation des secrets critiques

- Techniques d'accès à LSASS : credential dumping, manipulation mémoire
- Exploitation de DPAPI pour extraction de secrets utilisateurs et machine
- Kerberoasting avancé : récupération et cracking de TGS, analyse des erreurs de configuration

9 - Techniques de persistance sur AD

- Attaques via ADCS : émission frauduleuse de certificats, persistences basées sur les clés
- Manipulation des tickets Kerberos : golden, diamond, sapphire tickets
- Abus du mode DSRM, création de golden gMSA, réactivation silencieuse d'objets sensibles
- Abus AdminSDHolder, modification des ACL protégées
- Création de skeleton key, contournement des mécanismes d'authentification
- Empoisonnement de GPO : détournement de configuration à grande échelle
- Délégation Kerberos détournée pour persistance longue durée

10 - Extension de la compromission

- Analyse et exploitation des relations de confiance inter-domaines et inter-forêts
- Abus approfondi de la délégation Kerberos pour étendre la compromission au-delà du domaine initial

Les objectifs de la formation

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

Evaluation

- Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.

Les points forts de la formation

- Une immersion complète dans la sécurité offensive Active Directory
- Une expertise sur l’extraction de secrets critiques

Dates et villes 2026 - Référence SR389

Dernières places disponibles Session garantie

Rouen

du 30 mars au 2 avr.	du 24 août au 27 août	du 7 déc. au 10 déc.

A distance

du 30 mars au 2 avr.	du 24 août au 27 août	du 7 déc. au 10 déc.
du 8 juin au 11 juin	du 5 oct. au 8 oct.	

Toulouse

du 30 mars au 2 avr.	du 24 août au 27 août	du 7 déc. au 10 déc.

Paris

du 30 mars au 2 avr.	du 24 août au 27 août	du 7 déc. au 10 déc.
du 8 juin au 11 juin	du 5 oct. au 8 oct.	

Sophia Antipolis

du 30 mars au 2 avr.	du 24 août au 27 août	du 7 déc. au 10 déc.

Strasbourg

du 30 mars au 2 avr.	du 24 août au 27 août	du 7 déc. au 10 déc.

Rennes

du 8 juin au 11 juin	du 5 oct. au 8 oct.

Nantes

du 8 juin au 11 juin	du 5 oct. au 8 oct.

Lyon

du 8 juin au 11 juin	du 5 oct. au 8 oct.

Lille

du 8 juin au 11 juin	du 5 oct. au 8 oct.

Aix-en-Provence

du 8 juin au 11 juin	du 5 oct. au 8 oct.