Prendre le contrôle d'un Active Directory.

Vous faites déjà des tests d'intrusion et l'annuaire Windows vous résiste ? Du premier accès jusqu'au contrôle complet, puis l'art d'y rester sans se faire repérer. Quatre jours dans un environnement qui ressemble à celui de vos clients.

DURÉE	TARIF INTER	INTRA	NIVEAU
4 jours	**3 000 € HT**	**dès 1 500 € HT/jour**	**Avancé**

À l'issue de la formation

- Comprendre l'architecture d'Active Directory et les protocoles qui la portent
- Conduire une reconnaissance complète, depuis un accès anonyme puis authentifié
- Enchaîner des mouvements latéraux : relais NTLM, coercition d'authentification, abus de liens de confiance
- Élever ses privilèges localement et sur le domaine, jusqu'au contrôle de la forêt
- Extraire et rejouer les secrets d'un environnement compromis
- Installer et détecter des mécanismes de persistance durables
- Restituer les chemins d'attaque et les remédiations dans un rapport exploitable

Pour qui

- Pentesters et consultants en sécurité offensive
- Membres d'équipes red team et purple team
- Administrateurs Active Directory voulant auditer leur propre domaine
- Analystes SOC et CSIRT qui veulent comprendre les traces qu'ils voient passer
- Candidats aux certifications offensives orientées Active Directory

Prérequis

Administration Windows et Active Directory, notions réseau TCP/IP, aisance en ligne de commande Windows et Linux. Une première expérience de test d'intrusion est fortement recommandée : cette formation part du principe que la phase d'accès initial est acquise.

Déroulé

Jour 1 Fondations et reconnaissance

- Mécanismes d'administration : RPC, SMB, WMI, WinRM - ce que chacun expose
- Gestion des identités et des accès : NTLM et Kerberos, du ticket à l'usurpation
- Reconnaissance externe : OSINT sur les identifiants, les images, les adresses et les actifs exposés
- Reconnaissance interne depuis un accès anonyme, puis depuis un compte quelconque du domaine
- Techniques avancées de reconnaissance réseau et cartographie de la forêt
- TP : récupération d'identifiants, recherche de serveurs vulnérables via moteurs de recherche, espaces cloud exposés

Jour 2 Mouvements latéraux

- Empoisonnement ADIDNS et détournement de résolution de noms
- WinRM et JEA : ce que les restrictions d'administration laissent passer
- Extraction de secrets d'annuaire : LAPS, gMSA et sMSA
- Abus des liens de confiance MS-SQL et rebond entre serveurs
- Relais NTLM, coercition d'authentification, relais Kerberos
- Pivots inter-forêts, puis vers Azure (PHS, PTA, AD FS) et depuis Azure (Intune)
- TP : compromission d'un serveur par rejeu NTLM, prise de contrôle d'un MSSQL, élévation associée

Jour 3 Élévation de privilèges

- Élévation locale : jetons d'accès, usurpation, famille des vulnérabilités « potato »
- Contournement des restrictions logicielles : AppLocker, environnements Citrix verrouillés
- Élévation sur le domaine : étude et abus des ACL, chemins de contrôle
- Exploitation avancée des délégations Kerberos, contrainte et non contrainte
- Abus des services de certificats AD CS et des groupes privilégiés
- Kerberoasting, AS-REP roasting, rejeu d'authentification
- TP : identification et exploitation de chemins d'attaque avec BloodHound, du compte initial au domaine

Jour 4 **Extraction de secrets, persistance et restitution**

- Extraction de secrets critiques : LSASS, DPAPI, coffres et secrets applicatifs
- Persistance par certificats AD CS et par tickets Kerberos : golden, diamond, sapphire
- DSRM, golden gMSA, abus d'AdminSDHolder, skeleton key, empoisonnement de GPO
- Extension de la compromission : relations de confiance inter-domaines et inter-forêts
- Ce que chaque technique laisse comme trace, et comment un défenseur la voit
- Rédaction : chemins d'attaque, criticité, remédiations priorisées
- TP : compromission complète d'un domaine, Golden Ticket, skeleton key, DCSync

Ce qui est compris

- Laboratoire Active Directory multi-domaines avec relation de forêt
- Poste d'attaque Kali préconfiguré : Impacket, BloodHound, Certipy, Rubeus, mimikatz
- Scénarios de bout en bout avec corrigés commentés
- Grille de restitution des chemins d'attaque, réutilisable en mission
- Contrepartie défensive de chaque technique : ce qui la détecte, ce qui la bloque

Prochaines sessions inter-entreprises

DATES	LIEU ET FORMAT	PLACES
1 - 4 mars 2027	Paris · Présentiel ou distanciel	8 places
21 - 24 juin 2027	Paris · Présentiel ou distanciel	8 places
15 - 18 novembre 2027	À distance · Distanciel	8 places

Résistez aux hackeurs - organisme de formation certifié Qualiopi. Prise en charge OPCO possible, les pièces sont fournies.
Inscription et devis : https://resistez-aux-hackeurs.com/contact.html - formation@resistez-aux-hackeurs.com
Programme susceptible d'évoluer. Version du 08/10/2026. Accessibilité : nous contacter pour toute situation de handicap, nous étudions les adaptations possibles.