Pentest des environnements Active Directory : attaques et remédiation

Lien : https://innov-systems.com/formation/pentest-des-environnements-active-directory-attaques-et-remediation

DURÉE	RÉFÉRENCE	CATÉGORIE
5 jours (35h)	**SI112**	**Pentest**

Innov Systems

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Comprendre l’architecture et les failles d’Active Directory
- Identifier les vecteurs d’attaque sur les environnements AD
- Réaliser des tests d’intrusion sur un domaine Windows
- Exploiter les vulnérabilités d’authentification et de configuration
- Comprendre les techniques d’escalade de privilèges
- Simuler des attaques avancées (Kerberoasting, DCSync, etc.)
- Utiliser les outils de pentest AD (BloodHound, Mimikatz, Impacket)
- Évaluer la sécurité des contrôleurs de domaine
- Proposer des mesures de remédiation efficaces
- Améliorer la posture de sécurité des environnements d’identité
- Rédiger des rapports de pentest AD exploitables
- Étudier des scénarios réels de compromission de domaine

POUR QUI ?

- Pentesters / Ethical hackers
- Ingénieurs cybersécurité
- SOC analysts
- Administrateurs Active Directory
- Architectes IAM
- RSSI / CISO
- Consultants cybersécurité
- DevSecOps engineers
- Ingénieurs systèmes et réseaux
- Auditeurs sécurité IT
- Responsables infrastructure IT
- Toute personne impliquée dans la sécurité et l’audit des environnements Active Directory

Innov Systems

Programme détaillé

1 / Introduction au pentest Active Directory

- Rôle d’Active Directory dans les infrastructures d’entreprise
- Objectifs du test d’intrusion AD
- Surface d’attaque des environnements d’identité

2 / Cartographie et reconnaissance AD

- Énumération des domaines, forêts et trusts
- Analyse des utilisateurs, groupes et machines
- Collecte d’informations via LDAP, SMB et Kerberos

3 / Attaques sur les protocoles d’authentification

- Kerberoasting et AS-REP Roasting
- Pass-the-Hash et Pass-the-Ticket
- Attaques NTLM et relai d’authentification

4 / Exploitation des mauvaises configurations AD

- GPO mal sécurisées
- Permissions excessives et ACL faibles
- Délégations non sécurisées

5 / Escalade de privilèges dans Active Directory

- Exploitation des comptes à privilèges
- Abus des groupes sensibles (Domain Admins, Enterprise Admins)
- Techniques de privilege escalation locale et domaine

Innov Systems

6 / Attaques sur les contrôleurs de domaine

- DCSync et extraction de secrets AD
- Golden Ticket et Silver Ticket
- Compromission complète du domaine

7 / Mouvement latéral dans l’environnement AD

- Exploitation SMB et RDP
- Utilisation de PsExec et WMI
- Pivoting dans le réseau interne

8 / Outils de pentest Active Directory

- BloodHound et cartographie des relations AD
- Impacket suite
- Mimikatz et outils d’exploitation mémoire

9 / Détection et remédiation des attaques AD

- Durcissement des contrôleurs de domaine
- MFA et sécurité des comptes privilégiés
- Surveillance et détection des comportements anormaux

10 / Cas pratiques de pentest AD

- Simulation de compromission complète de domaine
- Analyse des vecteurs d’attaque
- Recommandations de correction et bonnes pratiques

Innov Systems

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

15 au 19 Fév. 2027	Présentiel - Casablanca
12 au 16 Avr. 2027	Présentiel - Casablanca
07 au 11 Juin 2027	Présentiel - Casablanca
02 au 06 Août 2027	Présentiel - Casablanca
27 Sep. au 01 Oct. 2027	Présentiel - Casablanca

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com

Innov Systems — Tous droits réservés