Sécurité offensive Active Directory : maîtrisez les techniques d’attaque et de défense des environnements Windows

Lien : https://innov-systems.com/formation/securite-offensive-active-directory-maitrisez-les-techniques-dattaque-et-de-defense-des-environnements-windows

DURÉE	RÉFÉRENCE	CATÉGORIE
5 jours (35h)	**SI53**	**Pentest**

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre l’architecture et les vulnérabilités de l’Active Directory
- Maîtriser les techniques de sécurité offensive en environnement Windows
- Savoir identifier et exploiter des failles de configuration AD
- Réaliser des attaques d’élévation de privilèges
- Comprendre les mécanismes d’authentification Windows
- Simuler des attaques de type red team sur un domaine
- Détecter les mouvements latéraux et compromissions
- Mettre en place des stratégies de défense adaptées
- Renforcer la sécurité globale des environnements Active Directory
- Développer une expertise en cybersécurité offensive

POUR QUI ?

- Pentesters et testeurs d’intrusion
- Experts en cybersécurité
- Administrateurs systèmes et réseaux
- Ingénieurs sécurité IT
- Responsables SOC et CERT
- Toute personne souhaitant se spécialiser en sécurité Active Directory

Innov Systems

Programme détaillé

1 / Introduction à l'Active Directory et à la sécurité offensive

- Rôle de l'Active Directory dans les systèmes d'information
- Principes de la sécurité offensive (red team)
- Enjeux de sécurité des environnements Windows

2 / Architecture et fonctionnement de l'Active Directory

- Domaines, forêts et contrôleurs de domaine
- Gestion des utilisateurs et des groupes
- Mécanismes d'authentification

3 / Reconnaissance et cartographie de l'environnement AD

- Collecte d'informations internes
- Analyse de la structure AD
- Identification des surfaces d'attaque

4 / Techniques d'élévation de privilèges

- Exploitation de mauvaises configurations
- Abus de privilèges utilisateurs
- Escalade locale et domaine

5 / Attaques sur les mécanismes d'authentification

- Kerberos et attaques associées
- Pass-the-Hash et Pass-the-Ticket
- Vol de credentials

Innov Systems

6 / Mouvement latéral dans le réseau

- Techniques de déplacement dans le domaine
- Exploitation des relations de confiance
- Compromission progressive du réseau

7 / Outils de sécurité offensive Active Directory

- Utilisation d’outils de pentest AD
- Frameworks d’attaque spécialisés
- Automatisation des tests de sécurité

8 / Persistence et maintien d’accès

- Techniques de persistance dans AD
- Création de portes dérobées logiques
- Contournement des mécanismes de sécurité

9 / Détection et réponse aux attaques AD

- Indicateurs de compromission
- Surveillance et logging
- Réponse aux incidents de sécurité

10 / Durcissement et remédiation de l’Active Directory

- Bonnes pratiques de sécurisation
- Réduction de la surface d’attaque
- Mise en place de politiques de sécurité renforcées

Inov 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

30 Nov. au 04 Déc. 2026	Présentiel - Casablanca
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

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