Sécurité offensive des infrastructures réseau pentest réseau et red teaming

Lien : https://innov-systems.com/formation/securite-offensive-des-infrastructures-reseau-pentest-reseau-et-red-teaming

DURÉE	RÉFÉRENCE	CATÉGORIE
10 jours (70h)	**SI64**	**Pentest**

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre les fondamentaux de la sécurité offensive réseau
- Maîtriser les techniques de pentest réseau
- Réaliser des simulations de red teaming
- Identifier et exploiter les vulnérabilités réseau
- Effectuer des mouvements latéraux dans un système compromis
- Analyser et compromettre des environnements Active Directory
- Utiliser des outils professionnels de pentest
- Rédiger des rapports d’audit de sécurité
- Simuler des attaques réalistes et avancées
- Comprendre les techniques d’évasion des défenses
- Améliorer la posture de sécurité des infrastructures
- Étudier des cas concrets d’intrusions réseau

POUR QUI ?

- Pentesters
- Ethical hackers
- Red teamers
- Ingénieurs cybersécurité
- Administrateurs systèmes et réseaux
- SOC analysts
- Consultants en sécurité offensive
- RSSI et responsables sécurité
- DevSecOps engineers
- Architectes sécurité
- Chercheurs en cybersécurité
- Toute personne impliquée dans la sécurité offensive des systèmes

Innov Systems

Programme détaillé

1 / Introduction à la sécurité offensive réseau

- Principes du hacking éthique
- Différence entre pentest et red teaming
- Objectifs des tests d’intrusion réseau

2 / Cartographie et reconnaissance réseau

- Collecte d’informations passives et actives
- Scan de réseaux et découverte d’hôtes
- Identification des surfaces d’attaque

3 / Analyse des protocoles réseau

- TCP/IP et protocoles critiques
- Vulnérabilités des services réseau
- Exploitation des mauvaises configurations

4 / Scan et énumération avancée

- Outils de scan réseau
- Énumération des ports et services
- Analyse des versions et failles connues

5 / Exploitation des vulnérabilités réseau

- Exploits courants sur services exposés
- Attaques sur protocoles non sécurisés
- Prise de contrôle initiale

Innov Systems

6 / Escalade de privilèges

- Techniques locales et réseau
- Abus de configurations système
- Exploitation de mauvaises permissions

7 / Mouvement latéral dans le réseau

- Techniques de propagation interne
- Exploitation des relations de confiance
- Compromission de segments réseau

8 / Attaques sur Active Directory

- Enumération AD
- Kerberos et attaques associées
- Domination de domaine

9 / Red teaming et simulation d’adversaires

- Simulation d’attaques avancées persistantes
- Scénarios réalistes d’intrusion
- Objectifs de compromission stratégique

10 / Évasion des mécanismes de défense

- Contournement des IDS/IPS
- Techniques d’obfuscation
- Anti-forensics

11 / Post-exploitation et maintien d’accès

- Persistance sur les systèmes compromis
- Création de backdoors

Inov Systems

- Extraction de données sensibles

12 / Outils de pentest réseau

- Nmap, Metasploit, Wireshark
- Frameworks de red teaming
- Automatisation des tests

13 / Reporting et documentation des attaques

- Rédaction de rapports techniques
- Classification des vulnérabilités
- Recommandations de remédiation

14 / Études de cas et exercices pratiques

- Scénarios de pentest complets
- Simulation de red team en environnement réel
- Analyse des résultats et remédiation

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

Innov Systems

Prochaines dates programmées

18 au 29 Jan. 2027	Présentiel - Casablanca
15 au 26 Mars 2027	Présentiel - Casablanca
10 au 21 Mai 2027	Présentiel - Casablanca
05 au 16 Juil. 2027	Présentiel - Casablanca
30 Août au 10 Sep. 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

Innov Systems