Lead Ethical Hacker : devenez expert en cybersécurité offensive et tests d’intrusion avancés

Lien : https://innov-systems.com/formation/lead-ethical-hacker-devenez-expert-en-cybersecurite-offensive-et-tests-dintrusion-avances

DURÉE
8 jours (56h)

RÉFÉRENCE
SI37

CATÉGORIE
Ethical Hacking

OBJECTIFS DE LA FORMATION

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

- Maîtriser les techniques avancées de hacking éthique
- Conduire des tests d’intrusion complets et structurés
- Identifier et exploiter les vulnérabilités systèmes et web
- Réaliser des attaques réseau et applicatives avancées
- Effectuer des opérations de post-exploitation
- Rédiger des rapports professionnels de pentest
- Diriger une équipe de red team efficacement
- Comprendre les mécanismes de défense pour mieux les contourner légalement
- Simuler des cyberattaques réalistes en environnement contrôlé
- Développer une expertise de niveau senior en cybersécurité offensive

POUR QUI ?

- Pentesters et hackers éthiques
- Experts red team
- Ingénieurs sécurité informatique
- Administrateurs systèmes et réseaux
- Analystes cybersécurité avancés
- Responsables sécurité (RSSI)
- Toute personne souhaitant évoluer vers un rôle de hacker éthique senior

Programme détaillé

1 / Introduction à l’éthique du hacking et au cadre légal

- Définition de l’éthique hacker
- Cadre juridique des tests d’intrusion
- Responsabilités du pentester senior

2 / Méthodologie avancée de test d’intrusion

- Frameworks (PTES, NIST, OWASP)
- Phases d’un pentest complet
- Planification et scoping des missions

3 / Reconnaissance et collecte d’informations avancée

- OSINT et intelligence open source
- Cartographie des cibles
- Analyse des surfaces d’attaque

4 / Scan et énumération des systèmes

- Détection des services et ports
- Identification des vulnérabilités
- Utilisation d’outils avancés de scan

5 / Exploitation des vulnérabilités

- Exploits web et systèmes
- Injection SQL et attaques applicatives
- Exploitation de failles connues

6 / Post-exploitation et élévation de privilèges

- Maintien de l’accès
- Escalade de privilèges
- Mouvement latéral dans le réseau

7 / Attaques sur réseaux et infrastructures

- Attaques MITM et sniffing
- Compromission réseau interne
- Exploitation Active Directory

8 / Sécurité des applications web avancées

- Analyse OWASP Top 10
- Tests sur API et microservices
- Sécurisation des applications modernes

9 / Contournement des mécanismes de sécurité

- Antivirus et EDR bypass
- Obfuscation et techniques stealth
- Anti-forensics

10 / Reporting et documentation professionnelle

- Rédaction de rapports de pentest
- Vulnérabilités et niveau de risque
- Recommandations de remédiation

11 / Gestion et leadership des équipes red team

- Coordination des missions offensives
- Gestion d’équipe de pentesters

- Stratégie d’attaque simulée

12 / Simulation complète de cyberattaque

- Scénarios réalistes d’intrusion
- Exercice red team vs blue team
- Analyse et débriefing complet

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

26 Oct. au 04 Nov. 2026 — 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