Maîtriser l’Ethical Hacking et la Cybersécurité Offensive

Lien :
https://innov-systems.com/formation/matriser-lethical-hacking-et-la-cybersecurite-offensive

DURÉE	RÉFÉRENCE	CATÉGORIE
4 jours (28h)	**SEC322**	**Ethical Hacking**

OBJECTIFS DE LA FORMATION

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

- Comprendre les principes fondamentaux de l’ethical hacking et les étapes d’un test d’intrusion complet
- Identifier, analyser et exploiter les vulnérabilités présentes dans les systèmes, réseaux et applications web
- Mettre en œuvre des techniques avancées de contournement, de post-exploitation et de protection
- Maîtriser les outils et méthodes de la cybersécurité offensive pour renforcer la défense des infrastructures
- Élaborer une stratégie d’audit et de sécurisation proactive adaptée à son environnement professionnel

POUR QUI ?

- Administrateurs systèmes et réseaux
- Responsables de la sécurité des systèmes d'information (RSSI)
- Ingénieurs et techniciens en cybersécurité
- Architectes d’infrastructure
- Chefs de projet techniques
- Responsables informatiques souhaitant renforcer la sécurité de leur SI

Programme détaillé

1 / FONDEMENTS DE L'ETHICAL HACKING

- Comprendre les principes, les cadres légaux et l'éthique du hacking
- Différences entre pentest, red teaming et audit de sécurité
- Les étapes d'un test d'intrusion : méthodologie et livrables

2 / COLLECTE D'INFORMATIONS ET FOOTPRINTING

- Techniques de reconnaissance passive (OSINT, whois, DNS, moteurs de recherche)
- Outils d'analyse de surface d'attaque : Maltego, Recon-ng, theHarvester
- Identification des cibles et cartographie du réseau

3 / ANALYSE ET ENUMÉRATION DES CIBLES

- Scanning réseau et détection d'hôtes avec Nmap et Masscan
- Identification de services, bannières et versions
- Enumération d'utilisateurs, partages et services ouverts

4 / VULNÉRABILITY SCANNING ET PRIORISATION

- Utilisation de scanners automatiques : OpenVAS, Nessus, Nikto
- Interprétation des rapports et hiérarchisation des risques
- Validation manuelle des vulnérabilités critiques

5 / EXPLOITATION DES VULNÉRABILITÉS

- Introduction à Metasploit Framework
- Exploitation des failles systèmes (Windows / Linux)
- Techniques d'élévation de privilèges et d'accès persistant

6 / POST-EXPLOITATION ET MAINTIEN D'ACCÈS

- Récupération d'informations sensibles
- Création de backdoors et pivoting réseau
- Effacement de traces et contre-mesures défensives

7 / HACKING D'APPLICATIONS WEB

- Vulnérabilités OWASP Top 10 : XSS, CSRF, File Inclusion, Command Injection
- Attaques sur les authentifications et gestion des sessions
- Analyse manuelle avec Burp Suite et exploitation avec scripts personnalisés

8 / ATTAQUES PAR INJECTION ET BASES DE DONNÉES

- SQL Injection avancée : détection, exploitation et automatisation
- Attaques NoSQL et contournement des filtres applicatifs
- Techniques de prévention et durcissement des bases de données

9 / HACKING DE RÉSEAUX ET PLATEFORMES MOBILES

- Analyse et attaque de protocoles sans fil (WEP, WPA2, WPA3)
- Attaques Man-in-the-Middle et interception de trafic
- Introduction au pentest mobile : architecture, émulation et reverse engineering

10 / ÉVASION ET CONTRE-MESURES

- Techniques d'évasion d'IDS, firewalls et antivirus
- Utilisation de chiffrages et tunnels pour la furtivité
- Détection et réponse aux intrusions (SOC mindset)

11 / HACKING DU CLOUD ET DES ENVIRONNEMENTS IoT

- Sécurité des environnements cloud (AWS, Azure, GCP)
- Exploitation des mauvaises configurations cloud

- Vulnérabilités et sécurisation des objets connectés (IoT/OT)

12 / BONNES PRATIQUES, STRATÉGIES ET CERTIFICATION

- Synthèse des apprentissages et retours d’expérience
- Élaboration d’une stratégie de défense en profondeur
- Préparation à la certification CEH et conseils de veille offensive

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

10 au 13 Nov. 2026	Distanciel

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