Maîtriser l’Ethical Hacking et les Tests d’Intrusion

Lien : https://innov-systems.com/formation/matriser-lethical-hacking-et-les-tests-dintrusion

DURÉE	RÉFÉRENCE	CATÉGORIE
5 jours (35h)	**SEC321**	**Ethical Hacking**

OBJECTIFS DE LA FORMATION

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

- Acquérir une compréhension approfondie des concepts, méthodologies et outils de l’ethical hacking moderne
- Développer des compétences pratiques en identification, exploitation et remédiation des vulnérabilités
- Mettre en œuvre des tests d’intrusion complets et documenter les résultats selon les standards professionnels
- Renforcer la posture de sécurité organisationnelle grâce à une approche proactive de la cybersécurité
- Se préparer à la certification CEH et aux exigences actuelles du marché de la sécurité offensive

POUR QUI ?

- Administrateurs systèmes et réseaux
- Responsables et ingénieurs en sécurité informatique
- Analystes SOC et auditeurs techniques
- Architectes IT impliqués dans la sécurité des infrastructures
- Chefs de projets techniques souhaitant comprendre les tests d’intrusion

Innov Systems

Programme détaillé

1 / INTRODUCTION À L'ETHICAL HACKING

- Définitions, enjeux et cadre légal
- Typologie des hackers et motivations
- Rôles et responsabilités de l'ethical hacker
- Bonnes pratiques éthiques et conformité (ISO 27001, RGPD)

2 / CADRE MÉTHODOLOGIQUE ET ENVIRONNEMENT DE TRAVAIL

- Étapes d'un test d'intrusion (PTES, OWASP, MITRE ATT&CK)
- Construction d'un lab de hacking (VM, réseaux isolés, outils)
- Choix et configuration des outils open source et commerciaux
- Gestion de projet et reporting d'audit de sécurité

3 / RECONNAISSANCE ET GATHERING D'INFORMATIONS

- Footprinting passif et actif
- Techniques de reconnaissance open source (OSINT)
- Outils : Maltego, theHarvester, Shodan, Recon-ng
- Analyse et cartographie des cibles

4 / SCANNING DES RÉSEAUX ET DÉTECTION DES SERVICES

- Découverte d'hôtes et de ports (Nmap, Masscan)
- Identification des services, versions et systèmes
- Analyse des bannières et fingerprinting avancé
- Détection d'intrusion et évasion de scans

5 / ENUMÉRATION ET IDENTIFICATION DES CIBLES

Innov Systems

- Énumération des utilisateurs, partages et services
- LDAP, SMB, SNMP, DNS et NetBIOS enumeration
- Vulnérabilités classiques et exploitation manuelle
- Scripts d’automatisation et exploitation basique

6 / ANALYSE ET EXPLOITATION DES VULNÉRABILITÉS

- Introduction aux CVE, CVSS et bases de vulnérabilités
- Analyse de vulnérabilités avec Nessus, OpenVAS, Nmap NSE
- Techniques d’exploitation avec Metasploit Framework
- Post-exploitation et élévation de privilèges

7 / HACKING DES SYSTÈMES ET POST-EXPLOITATION

- Exploitation locale et à distance
- Maintien d’accès et persistence
- Extraction de mots de passe et hash cracking
- Effacement de traces et dissimulation d’activités

8 / MALWARES, TROJANS ET BACKDOORS

- Analyse du fonctionnement des malwares
- Création et injection de backdoors
- Démystification des RATs et keyloggers
- Techniques de contournement des antivirus

9 / SOCIAL ENGINEERING ET PHISHING

- Psychologie de la manipulation et typologie d’attaques
- Création de campagnes de phishing contrôlées
- Ingénierie sociale en entreprise (tests de sensibilisation)
- Outils : SET, GoPhish, King Phisher

Inov Systems

10 / HACKING DES APPLICATIONS WEB

- Identification et exploitation des vulnérabilités OWASP Top 10
- Injection SQL, XSS, CSRF, LFI/RFI
- Tests de sécurité sur API REST et GraphQL
- Utilisation d’outils : Burp Suite, OWASP ZAP

11 / HACKING DES SERVEURS ET INFRASTRUCTURES WEB

- Attaques sur serveurs Apache, Nginx, IIS
- Vulnérabilités CMS (WordPress, Joomla, Drupal)
- Exploitation via fichiers uploadés et défauts de configuration
- Détection et mitigation des attaques

12 / ATTAQUES SUR RÉSEAUX SANS FIL

- Protocoles Wi-Fi et points de vulnérabilité
- Cracking WEP, WPA/WPA2 et attaques de désauthentification
- Sniffing et injection de paquets
- Sécurisation avancée des environnements Wi-Fi

13 / ÉVASION, IDS/IPS ET CONTRE-MESURES

- Techniques d’évasion de pare-feu et d’IDS
- Encodage, tunneling et spoofing
- Honeypots et détection de comportements suspects
- Bonnes pratiques de durcissement système

14 / CRYPTOGRAPHIE ET SÉCURISATION DES DONNÉES

- Principes fondamentaux de la cryptographie
- Chiffrement symétrique et asymétrique
- Attaques sur le chiffrement (Brute force, Rainbow tables)

Inov Systems

- Utilisation sécurisée des certificats et PKI

15 / PENTEST COMPLET ET RÉDACTION DE RAPPORT

- Conduite d’un test d’intrusion de bout en bout
- Analyse et synthèse des résultats
- Rédaction d’un rapport professionnel (technique et exécutif)
- Recommandations et plan d’action pour la 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

Prochaines dates programmées

18 au 22 Jan. 2027	Présentiel - Casablanca
15 au 19 Mars 2027	Présentiel - Casablanca
10 au 14 Mai 2027	Présentiel - Casablanca
05 au 09 Juil. 2027	Présentiel - Casablanca
30 Août au 03 Sep. 2027	Présentiel - Casablanca

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

Innov Systems

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