Tests d’Intrusion et Gestion des Vulnérabilités Réseau

Lien : https://innov-systems.com/formation/tests-dintrusion-et-gestion-des-vulnerabilites-reseau

DURÉE
5 jours (35h)

RÉFÉRENCE
SEC304

CATÉGORIE
Fondamentaux
Sécurité Informatique

OBJECTIFS DE LA FORMATION

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

- Comprendre le cadre légal, contractuel et organisationnel des tests d’intrusion
- Mettre en œuvre une méthodologie complète d’audit technique offensive
- Utiliser les principaux outils open source et professionnels de pentesting
- Identifier, exploiter et documenter les vulnérabilités réseau, système et applicatives
- Élaborer des rapports professionnels et proposer des plans de remédiation adaptés

POUR QUI ?

- Ingénieurs sécurité
- Administrateurs systèmes et réseaux
- Responsables SOC ou RSSI techniques
- Techniciens en sécurité informatique souhaitant se spécialiser dans le pentesting

Programme détaillé

1 / INTRODUCTION AU PENTEST ET À LA CYBERSÉCURITÉ OFFENSIVE

- Comprendre les finalités et les typologies de tests d'intrusion
- Cadre légal, éthique et contractuel du pentest
- Présentation des normes et référentiels : ISO 27001, NIST, OWASP

2 / PLANIFICATION ET DÉFINITION DU PÉRIMÈTRE

- Méthodologie de cadrage d'une mission
- Définition du périmètre, des objectifs et des contraintes
- Analyse de risques et autorisations nécessaires

3 / ENVIRONNEMENT DE TRAVAIL ET OUTILLAGE DU PENTESTER

- Préparation de la machine d'audit (Kali Linux, Parrot, VM, etc.)
- Découverte et configuration des outils essentiels : Nmap, Burp Suite, Metasploit
- Sécurisation du poste de test et gestion des logs

4 / RECONNAISSANCE ET EXPLORATION PASSIVE

- Techniques OSINT (Shodan, Whois, TheHarvester, Maltego)
- Analyse des empreintes numériques d'une organisation
- Cartographie du périmètre cible sans interaction directe

5 / EXPLORATION ACTIVE ET SCAN DE VULNÉRABILITÉS

- Découverte des hôtes et ports ouverts (Nmap avancé)
- Identification des services et bannières
- Scan de vulnérabilités avec OpenVAS et Nessus

6 / ENUMÉRATION ET IDENTIFICATION DES POINTS D’ENTRÉE

- Énumération des utilisateurs, partages et services
- Détection des systèmes d’exploitation et applications exposées
- Analyse des vulnérabilités exploitables

7 / EXPLOITATION DES VULNÉRABILITÉS RÉSEAU

- Attaques sur les protocoles réseau (ARP spoofing, DHCP, DNS, etc.)
- Exploitation des failles dans les réseaux câblés et Wi-Fi
- Introduction aux attaques MITM et à la capture de trafic

8 / EXPLOITATION DES VULNÉRABILITÉS SYSTÈME

- Exploitation sous Windows (failles SMB, RDP, privilèges locaux)
- Exploitation sous Linux (failles sudo, services mal configurés)
- Utilisation de Metasploit et modules spécifiques

9 / ATTAQUES SUR LES APPLICATIONS WEB

- Identification des failles OWASP Top 10
- Exploitation des vulnérabilités XSS, SQLi, CSRF, RCE
- Introduction au fuzzing et à la validation manuelle des résultats

10 / TECHNIQUES DE POST-EXPLOITATION

- Escalade de privilèges et persistance
- Collecte d’informations sensibles et extraction de données
- Effacement des traces et couverture opérationnelle

11 / ATTAQUES AVANCÉES ET MOUVEMENTS LATÉRAUX

- Déploiement de payloads et pivot réseau
- Exploitation via PowerShell Empire, CrackMapExec, BloodHound

- Simulation d’attaques internes (Red Team basics)

12 / UTILISATION DE SCRIPTS ET AUTOMATISATION

- Introduction aux scripts d’audit (Bash, Python, PowerShell)
- Automatisation de scans et de rapports
- Génération de scripts personnalisés pour la collecte de données

13 / ANALYSE ET INTERPRÉTATION DES RÉSULTATS

- Consolidation et hiérarchisation des vulnérabilités
- Analyse des impacts métiers et techniques
- Priorisation des risques selon leur criticité

14 / RÉDACTION DU RAPPORT DE PENTEST

- Structuration d’un rapport professionnel (technique + exécutif)
- Bonnes pratiques de communication des résultats
- Présentation au client et gestion de la phase post-audit

15 / PLAN D’ACTION ET DÉFENSE PROACTIVE

- Élaboration d’un plan de remédiation
- Introduction à la défense en profondeur
- Bonnes pratiques pour renforcer la posture de sécurité

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

20 au 24 Juil. 2026	Présentiel - Casablanca
14 au 18 Sep. 2026	Distanciel
09 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