KIN TRAINING · FORMATION & CERTIFICATION

Hacking éthique et tests d'intrusion : les fondamentaux

Adoptez le point de vue de l'attaquant pour mieux défendre vos systèmes.

CY-PENTEST | Avancé | Formation

Description

Cette formation offensive et pratique, menée en environnement de laboratoire cloisonné, parcourt les phases d'un test d'intrusion : reconnaissance, scan, exploitation et post-exploitation, sur des cibles vulnérables volontairement mises à disposition. L'objectif est strictement défensif : comprendre les techniques d'attaque pour renforcer la sécurité, dans un cadre légal et éthique.

Informations

Durée
4 jours

Domaine
Cybersécurité

Formats
Présentiel, Distanciel, Blended

Langue
Français

Objectifs

- Comprendre la méthodologie et le cadre légal d'un test d'intrusion
- Mener une reconnaissance et cartographier une surface d'attaque
- Identifier et comprendre l'exploitation des vulnérabilités courantes
- Rédiger un rapport de test d'intrusion et recommander des remédiations

Prérequis

- Bonnes connaissances en réseaux TCP/IP et systèmes Linux/Windows
- Notions de sécurité des SI

Public visé

- Consultants et analystes en cybersécurité
- Administrateurs et ingénieurs sécurité
- Auditeurs techniques

Programme détaillé

01. Cadre et méthodologie

- Cadre légal, éthique et règles d'engagement
- Méthodologies (PTES, OWASP) et types de tests
- Mise en place du laboratoire

02. Reconnaissance et scan

- OSINT et collecte d'informations
- Découverte réseau et cartographie
- Scan de ports, de services et de vulnérabilités

03. Exploitation

- Vulnérabilités web courantes (OWASP Top 10)
- Failles systèmes et élévation de privilèges
- Comprendre les frameworks d'exploitation

04. Post-exploitation et reporting

- Persistance et mouvement latéral : principes
- Nettoyage et preuve de concept
- Rédaction du rapport et plan de remédiation