INTRA

INTER

INITIATION AUX PENTESTS (TESTS D'INTRUSION)

COMPRENDRE, RÉALISER ET EXPLOITER LES TESTS D'INTRUSION DANS UNE DÉMARCHE DE CYBERSÉCURITÉ OPÉRATIONNELLE

OBJECTIFS

1. Comprendre les concepts fondamentaux du pentest (test d'intrusion) et son rôle dans une démarche globale de cybersécurité.
2. Identifier les différentes phases d'une campagne de pentest, de la reconnaissance à l'exploitation, en passant par la post-exploitation et le reporting.
3. Acquérir une maîtrise opérationnelle des méthodologies et outils utilisés lors d'un test d'intrusion, en environnement réseau, applicatif ou système.
4. Savoir structurer et documenter un rapport de pentest professionnel, en mettant en avant les vulnérabilités identifiées, leur criticité et les recommandations associées

MOYENS PÉDAGOGIQUES

Projection du cours, support de cours papier, clés USB et VM (machines virtuelles)
Chaque point de la formation sera illustré par des exemples concrets afin que les participants puisse s'approprier le sujet.

MÉTHODES UTILISÉES

La progression pédagogique du participant est évaluée tout au long de la formation au moyen de QCM.

PUBLIC

> Responsables SSI, administrateurs systèmes et réseaux, ingénieurs cybersécurité. Développeurs, techniciens ou chefs de projet souhaitant comprendre les tests d'intrusion.
Professionnels IT avec une première culture sécurité, impliqués dans la protection des systèmes d'information

PRIX HT
À partir de 1 300 €

DATES
17 et 18 mars 2026

DURÉE
2 jours (14 heures)

LIEU
LCIE

INTERVENANT
Expert en cybersécurité

PRÉ-REQUIS
Compréhension des principaux concepts et termes en cybersécurité
Notions de base en réseaux (TCP/IP, ports, protocoles)

PARCOURS DE FORMATION

> Introduction aux tests d'intrusion
- Définitions, objectifs et cadre légal
- Typologie des tests : boîte noire, boîte grise, boîte blanche
- Méthodologies : OWASP, PTES

> Méthodologie d'un pentest
- Phase de reconnaissance (OSINT, scan réseau)
- Cartographie et énumération des services
- Identification des vulnérabilités (automatisée et manuelle)
- Exploitation des failles courantes (injections, accès non autorisé)
- Post-exploitation, élévation de privilèges, maintien d'accès
- Rédaction d'un rapport de test clair et exploitable

> Outils et démonstrations
- Présentation des principaux outils : Nmap, Burp Suite, Metasploit, etc.
- Exemples de scénarios sur un environnement de test dédié
- Lecture et interprétation de rapports de scan (Nessus)

> Analyse et recommandations
- Exploiter les résultats pour améliorer sa posture sécurité
- Priorisation des vulnérabilités (CVSS, risque métier)
- Lien avec la gestion des risques cybersécurité de l'entreprise