+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 22/08/2025

S'inscrire

Formation Pentesting - Réaliser des tests d'intrusion

5 jours (35 heures)

Présentation

Les tests d'intrusion (ou pentests) sont aujourd'hui l'outil de référence pour valider la robustesse d'un système d'information face aux cyber-menaces toujours plus sophistiquées. Cette formation « Pentesting : Réaliser des tests d'intrusion » vous donnera les compétences nécessaires pour identifier, exploiter et corriger les vulnérabilités tout en respectant le cadre juridique français (loi Godfrain, LCEN) et européen (NIS 2, RGPD).

Au cours de cette formation, vous découvrirez les fondamentaux du pentesting et son positionnement dans la gestion du risque, tout en intégrant les dimensions légales, éthiques et organisationnelles propres à la discipline. Vous apprendrez à planifier une mission, à définir un périmètre d'intervention et à collecter les informations nécessaires grâce à l'OSINT et aux techniques de reconnaissance.

Vous serez guidés dans l'utilisation d'outils et méthodes de pointe pour le scan, l'analyse de vulnérabilités, l'exploitation d'applications web, de réseaux et de systèmes, mais aussi pour la post-exploitation, le mouvement latéral et l'exfiltration de données. Les attaques client-side et l'ingénierie sociale seront également abordées pour compléter votre compréhension des vecteurs de compromission modernes.

Une place importante sera donnée à la méthodologie et à la restitution : rédaction de rapports d'audit clairs, construction de preuves d'exploitation (POC) et formulation de recommandations concrètes à destination des équipes techniques et managériales.

Comme pour toutes nos sessions, ce programme s'appuie sur la dernière version stable des outils et intègre les CVE critiques de 2025, pour une veille et des pratiques toujours à jour.

Objectifs

- Comprendre les fondamentaux et le cadre juridique du pentesting

- Connaître les différentes phases d'un test d'intrusion
- Utiliser les outils et techniques d'analyse de pentesting
- Simuler des attaques
- Rédiger un rapport d'audit professionnel

Public visé

- RSSI
- Techniciens
- Auditeurs amenés à faire du pentest
- Administrateurs systèmes et réseaux

Pré-requis

- Des notions en informatique et sécurité des systèmes d'information

Programme de notre Formation Pentesting

[Jour 1 - Matin]

Panorama du pentesting et des menaces

- Définition des tests d’intrusion ; black-, grey-, white-box
- Acteurs & motivations : cyber-crime, hacktivisme, espionnage
- Positionnement du pentest dans la gestion du risque (ISO 27005)
- Comprendre les fondamentaux du pentesting
- Atelier pratique : Cartographier la surface d’attaque d’un SI fictif.

[Jour 1 - Après-midi]

Cadre légal, conformité et éthique

- Législation FR (LCEN, loi Godfrain) & UE (NIS 2, RGPD) applicables
- Responsabilités pénales/civiles ; accords de confidentialité (NDA)
- Normes & référentiels : PTES, OSSTMM, ISO/IEC 17025
- Comprendre le cadre juridique pour mener des tests conformes et maîtrisés
- Atelier pratique : Analyser une lettre de mission et identifier les clauses critiques.

Scoping et planification de la mission

- Collecte des exigences client, périmètre & objectifs
- Analyse de risque : contraintes techniques, planning, ressources

- Choix des approches : black-box vs grey-box vs white-box
- Atelier pratique : Élaborer un plan de test et un RACI simplifié.

[Jour 2 - Matin]

OSINT et reconnaissance passive

- WHOIS, Shodan, archives DNS, réseaux sociaux
- Extraction de métadonnées & Google dorks
- Cartographie initiale des actifs / priorisation des cibles
- Atelier pratique : Extraire des infos sur une cible publique via SpiderFoot.

[Jour 2 - Après-midi]

Scan actif & énumération réseau

- Discovery réseau : Nmap, Masscan, fingerprinting
- Banner grabbing & détection de versions
- Identification d’équipements sans fil / IoT
- Atelier pratique : Réaliser un scan Nmap complet et interpréter les résultats.

Analyse de vulnérabilités

- Scanners automatiques (Nessus, OpenVAS) vs analyse manuelle
- Notation CVSS ; corrélation avec la criticité métier
- Gestion des faux positifs / faux négatifs
- Atelier pratique : Qualifier les vulnérabilités critiques d’un rapport OpenVAS.

[Jour 3 - Matin]

Exploitation d’applications web

- OWASP Top 10 : SQLi, XSS, SSRF, etc.
- Outils : Burp Suite Pro, SQLmap ; contournement WAF
- Escalade de privilèges logiques (IDOR, logique métier)
- Atelier pratique : Exploiter une faille XSS stockée dans Juice Shop.

[Jour 3 - Après-midi]

Exploitation réseau & système

- Exploits distants (SMB, RDP) & Metasploit
- Buffer overflow modernes (ROP, ASLR bypass)
- Password cracking, pass-the-hash, Kerberoasting
- Simuler des attaques réalistes pour tester la résilience d’un système d’information.
- Atelier pratique : Compromission d’un serveur Windows via EternalBlue.

Ingénierie sociale & attaques client-side

- Phishing / spear-phishing : kits, métriques de succès
- Attaques macro, HTA, USB Rubber Ducky
- Contournement EDR basiques
- Atelier pratique : Lancer une campagne de phishing dans un lab GoPhish.

[Jour 4 - Matin]

Post-exploitation et escalade de privilèges

- Enumeration locale avancée (LinPEAS, WinPEAS)
- Exploitation de services faibles, tâches planifiées, CVE locales
- Pillage de credentials (LSASS, SAM, Mimikatz)
- Atelier pratique : Obtenir SYSTEM sur une VM vulnérable.

[Jour 4 - Après-midi]

Mouvement latéral & persistance

- Pass-the-Ticket, WMI, PsExec, SSH trust
- Backdoors : tâches planifiées, registre, cron
- Techniques d’évasion & OPSEC pendant l’intrusion
- Atelier pratique : Pivoter vers un sous-réseau via proxychains.

Exfiltration & nettoyage

- Exfiltration : DNS tunnelling, HTTPS covert channel
- Compression, chiffrement, stéganographie des données
- Anti-forensic : effacement de logs & artefacts
- Atelier pratique : Exfiltrer des documents via un canal DNS chiffré.

[Jour 5 - Matin]

Simulation d’attaque end-to-end

- Mise en place d’un C2 (Cobalt Strike / Sliver)
- Chaîne complète : recon, exploit, C2, exfiltration
- Collecte d’IOCs & génération de logs pour blue-team
- Atelier pratique : Challenge CTF chronométré « Capture The Flag ».

[Jour 5 - Après-midi]

Élaboration du rapport d’audit

- Structure : executive summary, findings, POC, remédiations
- Métriques : CVSS, kill-chain, mapping MITRE ATT&CK
- Plan d’action priorisé & quick wins
- Rédiger un rapport d’audit professionnel clair et exploitable par les équipes techniques et décisionnaires.
- Atelier pratique : Rédiger une fiche de vulnérabilité critique en peer-review.

Debriefing & amélioration continue

- Présentation orale des résultats ; gestion des questions sensibles
- Frameworks de maturité : OSCP, NIST, purple-teaming
- Capitalisation : scripts réutilisables & veille vulnérabilités
- Atelier pratique : Rétrospective d’équipe & plan d’amélioration continue.

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des

séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.