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

Mis à jour le 05/08/2025

S'inscrire

Formation Pentesting - Réaliser des tests d'intrusion

5 jours (35 heures)

Présentation

Maîtrisez les tests d'intrusion de bout en bout avec cette formation complète en pentest, conçue pour les professionnels IT, DevSecOps et experts cybersécurité. Vous apprendrez à planifier, exécuter et documenter des tests efficaces sur des infrastructures variées, en respectant les cadres légaux et les bonnes pratiques.

Vous débuterez par la reconnaissance passive et active, avec les outils et techniques OSINT, la cartographie réseau, l'énumération de services et les scans de vulnérabilités.

Vous apprendrez ensuite à exploiter des failles sur les couches web, réseau et système, à utiliser Metasploit, à élever vos privilèges et à maintenir un accès post-exploitation en environnement Windows et Linux.

La formation vous fera progresser sur les attaques avancées : Active Directory, conteneurs Docker/K8s, techniques d'évasion, et scénarios multi-vecteurs en environnement simulé.

Comme pour toutes nos formations, celle-ci vous sera présentée avec les toutes dernières actualisations en matière de Pentesting.

Objectifs

- Comprendre les objectifs, types, cadres légaux et méthodologies des tests d'intrusion
- Identifier, cartographier et analyser les cibles via des techniques de reconnaissance passive et active
- Exploiter les vulnérabilités web, réseau, système et Active Directory à l'aide d'outils dédiés
- Élever les privilèges, maintenir l'accès et contourner les mécanismes de détection et de sécurité
- Rédiger un rapport de pentest structuré avec évaluation des risques et recommandations de remédiation
- Valider les compétences par la réalisation d'un test d'intrusion complet sur un environnement simulé

Public visé

- DévSecOps
- Pentester

Pré-requis

- connaissance des systèmes Linux et Windows
- Maîtrise des bases réseau

Programme de la formation JUnit : Test Java efficace

Introduction au pentest

- Définition, objectifs, périmètres (web, infra, mobile, IoT…)
- Différences entre Pentest, Red Team, Audit de vulnérabilités
- Types de tests (boîte noire, grise, blanche)
- Cadre légal et éthique

Préparer un test d’intrusion

- Comprendre les objectifs et périmètre du client
- Rédiger une lettre de mission
- Choix des outils et méthodologie

Reconnaissance passive

- OSINT
- Analyse DNS
- Recherche de leaks

Reconnaissance active

- Scan de port
- Détection de services et bannières
- Fingerprinting OS
- Scan de vulnérabilités

Enumération avancée

- Enumération SMB, LDAP, FTP, SNMP
- Analyse NetBIOS / Kerberos
- Enumération Web
- Enumération de réseau interne

Pentest Web – Introduction

- OWASP Top 10 : panorama des failles majeures
- Fuzzing avec wfuzz, ffuf, Dirb
- Détection de technologies

Attaques Web classiques

- Injection SQL
- Command Injection / RCE
- File Inclusion
- Cross-Site Scripting
- Cross-Site Request Forgery

Automatisation des attaques web

- Burp Suite
- ZAP Proxy
- Nikto / wapiti / OWASP ZAP CLI

Exploitation réseau et services

- Vulnérabilités SMB

- Vulnérabilités FTP, RDP, Telnet
- Exploitation DNS
- Man-in-the-Middle

Prise de contrôle système

- Exploits publics
- Metasploit Framework
- Reverse shell et bind shell
- Post-exploitation avec Metasploit

Escalade de privilèges

- Enumération système
- Privilèges SUID, Scheduled Tasks, Unquoted Service Path
- Exploitation des failles locales
- Pillage de credentials

Persistences et nettoyage

- Techniques de persistance
- Rootkits et shells persistants
- Effacement des traces

Attaque d’un environnement Active Directory

- Enumération AD
- Kerberoasting / AS-REP roasting
- Pass-the-Hash / Pass-the-Ticket / Golden Ticket
- Exploitation GPO, ACL, délégations

Sécurité des conteneurs

- Introduction à Docker et Kubernetes
- Vulnérabilités fréquentes

- Breakout de conteneur vers hôte
- Outils : Dockerscan, kube-hunter

Techniques d’évasion

- Antivirus Evasion
- Bypasser l’EDR : LOLBAS, living-off-the-land
- Payloads personnalisés avec msfvenom / Veil / Unicorn

Réaliser un test multi-vecteurs

- Scénario d’attaque combinée : web ? RCE ? reverse shell ? AD
- Approche Red Team sur un lab simulé

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.