New

Pentesting - Réaliser des tests d'intrusion

Identifier les failles pour renforcer la sécurité des systèmes

Présentiel ou en classe à distance

5 jours (35 h)

Prix inter : 3.890,00 € HT
Forfait intra : 10.990,00 € HT

Réf.: SE116

La formation **Pentesting Réaliser des tests d'intrusion** offre une approche complète et opérationnelle pour maîtriser les **méthodologies, outils et techniques du pentest** dans un cadre professionnel et légal. Elle couvre l'ensemble du cycle d'un test d'intrusion : reconnaissance passive (OSINT), cartographie réseau, scan de vulnérabilités, exploitation, post-exploitation, élévation de privilèges et reporting. Les participants apprennent à utiliser les outils de référence du domaine tels que Kali Linux, Nmap, Metasploit, Shodan, theHarvester, Meterpreter et à analyser les vulnérabilités selon les standards OWASP, NIST et PTES. Les ateliers pratiques permettent de simuler des attaques réalistes sur des environnements contrôlés, afin de comprendre concrètement les techniques utilisées par les attaquants.
Au-delà des aspects techniques, la formation met l'accent sur le **cadre juridique et éthique du pentesting**, la rédaction d'une lettre de mission, la gestion des autorisations et la production de **rapports d'audit professionnels** incluant preuves de concept et recommandations. Les apprenants développent ainsi une vision complète du métier de pentester, de la phase d'audit jusqu'à la restitution des résultats au client.

A qui s'adresse cette formation ?

Pour qui

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

Prérequis

- Des notions en informatique et sécurité des systèmes d'information
- Disposez-vous des connaissances nécessaires pour suivre cette formation ? Testez-vous !

Programme

1 - Fondamentaux du Pentesting

- Définitions et concepts clés
- Types de tests d'intrusion (Black box, White box, Gray box)
- Différence entre pentest et audit de vulnérabilités
- Acteurs et rôles (Red Team, Blue Team, Purple Team)
- Standards et référentiels (PTES, NIST, OWASP)

Atelier

Prise en main de Kali Linux VM

Configuration lab Metasploitable

2 - Cadre et méthodologie du Pentesting

- Aspects éthiques et rôle du "hacker éthique"
- Cybersécurité responsable et protection des parties prenantes
- Le cadre légal : le mandat d'audit et les responsabilités

- Autorisations, contrats et chartes éthiques
- Méthodologies de test d’intrusion : reconnaissance, scan, exploitation, post-exploitation, rapport

Atelier

Analyse contrat type, rédaction lettre de mission

3 - Reconnaissance passive (OSINT)

- Techniques de renseignement en sources ouvertes (OSINT)
- Recherche d'informations sur les sites web, les réseaux sociaux, les forums, etc
- Utilisation des moteurs de recherche avancés (Google Dorks)
- Présentation des outils de reconnaissance passive

Atelier

Utilisation d'outils comme theHarvester pour trouver des adresses e-mail et des noms d'hôtes

Utilisation de Shodan pour identifier des serveurs exposés

4 - Reconnaissance active et cartographie du réseau

- Introduction au balayage de ports et aux types de scans (TCP, UDP)
- Analyse des en-têtes de paquets avec des outils de capture réseau
- Le rôle des pare-feu et leur contournement

Atelier

Utilisation avancée de Nmap pour le balayage de ports, la détection de services, la reconnaissance du système d'exploitation et l'utilisation de scripts NSE

5 - Scan de vulnérabilités

- Définition d'une vulnérabilité et d'un exploit
- Présentation des scanners de vulnérabilités comme Nmap et leur fonctionnement
- Interprétation des rapports de scan et hiérarchisation des risques (CVSS)

Atelier

Lancement d'un scan de vulnérabilités sur les machines cibles, analyse des résultats et identification des failles critiques

6 - Exploitation et Metasploit

- Les différents types d'exploits (dépassement de tampon, injections SQL, etc.)
- Présentation des frameworks d'exploitation, avec un focus sur Metasploit
- Architecture de Metasploit : modules, payloads, listeners, etc

Atelier

Lancement d'une attaque simple avec Metasploit pour exploiter une vulnérabilité et obtenir un shell Meterpreter

7 - Exploitation de services et d'applications

- Exploitation de services réseau (FTP, SSH, telnet, etc.)
- Attaques sur les applications web (injections SQL, XSS)

Atelier

Exploitation de différentes failles (vsftpd, Apache Tomcat, etc.) sur la machine virtuelle Metasploitable

8 - Post-exploitation et maintien d’accès

- Techniques de post-exploitation : collecte d’informations internes, pivotement vers d’autres machines, etc
- Maintien d’accès (création de backdoors, rootkits)
- Présentation de la boîte à outils Meterpreter

Atelier

Utilisation de Meterpreter pour énumérer le système, collecter des informations (fichiers de configuration, mots de passe), et se déplacer sur le réseau interne

9 - Élévation de privilèges

- Stratégies d'escalade de privilèges sur Linux et Windows
- Recherche de failles dans la configuration (permissions incorrectes, services vulnérables)

Atelier

Identification d'une méthode d'escalade de privilèges sur un système vulnérable (par exemple, via un service mal configuré ou un binaire avec le bit

SUID) et application de l'attaque

10 - De l'audit au rapport

- Importance du rapport d'audit pour le client
- Structure d'un rapport de test d'intrusion (résumé exécutif, méthodologie, vulnérabilités découvertes, recommandations techniques et stratégiques)
- Critères de qualité pour un rapport professionnel
  Atelier

  Rédaction d’une section de rapport d'audit pour une vulnérabilité découverte et exploitée lors de la formation, en incluant une description, une preuve de concept et des recommandations

11 - Synthèse

- Récapitulatif des phases du pentest
- Bonnes pratiques et éthique continue du pentesting
- Impact global de la cybersécurité sur la durabilité numérique
- Présentation des certifications existantes
  Atelier

  Réalisation d’un test d'intrusion complet (de la reconnaissance au reporting) sur une nouvelle cible vulnérable

Après la session

- Sécurité informatique, concepts essentiels et techniques de protection pour l'utilisateur

Les objectifs de la formation

- 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

Evaluation

- Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.

Les points forts de la formation

- L'apprentissage par la pratique : les phases théoriques sont complétées d'ateliers favorisant un ancrage durable des acquis
- Les nombreux retours d'expérience et conseils des consultants spécialistes du sujet
- Utilisation d'environnements proches du contexte professionnel

Dates et villes 2026 - Référence SE116

Dernières places disponibles Session garantie

A distance

du 9 mars au 13 mars	du 22 juin au 26 juin	du 19 oct. au 23 oct.
du 18 mai au 22 mai	du 31 août au 4 sept.	du 23 nov. au 27 nov.

Paris

du 9 mars au 13 mars	du 22 juin au 26 juin	du 19 oct. au 23 oct.
du 18 mai au 22 mai	du 31 août au 4 sept.	du 23 nov. au 27 nov.