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

Mis à jour le 25/03/2025

S'inscrire

Formation Certification CompTIA Pentest+ (PT0-002)

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

5 jours (35 heures)

Présentation

Notre formation Comptia Pentest+© vous préparera efficacement au passage de la certification. Cette certification vous permettra de prouver vos compétences en test d'intrusion et en sécurité informatique, renforçant ainsi votre crédibilité et votre valeur sur le marché professionnel.

Notre formation couvre l’ensemble des compétences nécessaires pour identifier, exploiter et documenter les vulnérabilités des systèmes, réseaux et applications.

La formation vous offre une expertise complète pour réussir l’examen PT0-002 tout en développant des compétences directement applicables en entreprise.

Nous mettons constamment à jour notre programme pour refléter les dernières évolutions de l'industrie et assurer que nos apprenants disposent des compétences les plus récentes.

Contenu de la formation

- 4 jours de formation avec un expert certifié
- 1 an d'accès aux Labs en autoformation
- 1 passage de la certification

Objectifs

- Comprendre les principes fondamentaux des tests d'intrusion et des cadres réglementaires associés (RGPD, PCI DSS)

- Savoir planifier, exécuter et documenter un test d'intrusion, depuis la collecte jusqu'à la remédiation
- Exploiter des vulnérabilités réseau, applicatives et système en utilisant des outils professionnels (Nmap, Nessus, Metasploit, etc.).
- Maîtriser la rédaction de rapports clairs et exploitables pour différents publics (techniques et non techniques).
- Développer des compétences en communication et en rédaction de rapports

Public visé

- Pentesters
- Analystes en cybersécurité
- Consultants en sécurité
- Administrateurs systèmes

Pré-requis

- 3 à 4 ans d'expérience pratique dans la réalisation des tests d'intrusion, des évaluations de vulnérabilité et l'analyse de code
- Connaissances solides en sécurité informatique
- Avoir des notions fondamentales sur les tests d'intrusion
- Connaissances en langages de script comme Python ou Ruby

Pré-requis logiciels

- Environnement de virtualisation (VMware ou VirtualBox)
- Outils de test de vulnérabilité (Nmap, Metasploit, Burp Suite, OWASP ZAP, SQLmap...)
- Outils de gestion de mots de passe et de stockage sécurisé des informations sensibles

Note : Ambient IT n’est pas propriétaire de Comptia Certifications©, cette certification appartient à Comptia®, Inc.

Programme de la Préparation à la Certification Pentest+©

Introduction à la cerification PenTest+

- Objectifs de la certification PenTest
- Principes fondamentaux des tests d'intrusion
- Présentation des outils et environnements nécessaires

Plannification et Scoping

- Comprendre les cadres réglementaires (RGPD, PCI DSS)
- Règles d'engagement et contraintes légales
- Définir les périmètres et les cibles des tests
- Élaboration d'une stratégie adaptée (test en environnement connu et inconnu)

Collecte d'informations et d'analyse des vulnérabilités

- **Techniques d'OSINT (recherche d'informations publiques)**
- Analyse des cibles : réseau, applications, cloud
- **Utilisation et priorisation de vulnérabilités (CVE, CWE)**

Exploitation et attaques

- Techniques d'exploitation réseau (ARP spoofing, VLAN hopping)
- Attaques sur les applications web (injection SQL, XSS, API)
- Exploitation des vulnérabilité mobiles et IoT
- Post exploitation : persistance et mouvements latéraux

Rapport et remédiations

- Rédaction de rapports adaptés aux audiences techniques et non techniques
- Recommandations pour la remédiations des vulnérabilités
- Technique de durcissement des systèmes et bonne pratiques (patch management, MFA)
- Rédaction et présentation d'un rapport final

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.