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

Mis à jour le 20/03/2025

S'inscrire

Formation Certification CPTS

All-In-One : Préparation & Examen inclus au tarif

3 jours (21 heures)

Présentation

Notre formation Certification CPTS vous permettra de valider vos compétences pratiques et techniques en sécurité offensive et de devenir pentester. Le test d'intrusion, est la pratique qui consiste à identifier, exploiter et documenter les vulnérabilités afin sécuriser votre infrastructures informatiques.

Notre programme de formation enseignera toutes les étapes et les techniques d'une analyse Pentesting et vous permettra, à l'issue de ces 3 jours, de passer l'examen de certification CPTS.

À l'issue de cette formation, vous saurez identifier, exploiter et documenter les vulnérabilités et proposer des solutions pour renforcer et d'optimiser la sécurité.

Objectifs

- Comprendre les concepts fondamentaux du pentesting.
- Identifier et énumérer efficacement les vulnérabilités techniques d'une organisation.
- Maîtriser l'exploitation concrète des failles identifiées.
- Conduire des tests avancés sur les applications web et systèmes internes.
- Proposer des recommandations pertinentes pour sécuriser durablement les infrastructures.
- Préparer et réussir l’examen officiel de certification CPTS.

Public visé

- Pentesters
- Analystes en cybersécurité
- Consultants en sécurité

- Administrateurs systèmes

Pré-requis

- Connaissances solides en sécurité informatique
- Avoir des notions fondamentales sur les tests d’intrusion
- Connaissances en langages de script comme Python ou Ruby

Programme de notre Formation Certification CPTS

Reconnaissance et la collecte d'information ciblées

- Approche résaux avec Nmap
- Enumération du DNS et sous-domaines
- Identifier les version vulnérable et Fingerprinting du système
- SMB & FTP

Identification et exploitation de vulnérabilités

- Introduction aux exploits publics, Metasploit Framework
- Recherche de vulnérabilités :
  - buffer
  - overflow
  - basiques
- Exploitation de vulnérabilités Web courantes
- Shells inversés et bind shells
- Techniques de transfert de fichiers malveillants

Tests Avancés Sécurité des Applications Web

- SQLi (Injection SQL), XSS (scripting)
- Inclusion de fichiers LFI/RFI et Attaques CSRF
- Tests de sécurité avec Burp Suite
- Manipulation avancée des requêtes HTTP
- **FFUF**

Post-exploitation & Privileges

- Escalade de privilèges avec Linux
- Escalade de privilèges avec Windows
- Techniques de maintien des accès
- Extraction des mots de passe/hashes

- Tunneling SSH, Pivoting réseau

Intrusions avancées en environnement Active Directory

- Fondamentaux d'Active Directory
- Énumération Active Directory avec BloodHound
- Attaque Pass-the-Hash et Exploitation Kerberos
  - Kerberoasting
  - Golden Ticket
- LDAP

Rapport & méthodologie Pentest

- Conseils et révisions en vue de l'examen
- Méthodologie standard OWASP/PTES
- Classification des vulnérabilités (CVSS)
- Présentation des résultats techniques

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.