

CompTIA PenTest+

Réf. G015 · CompTIA · Cybersécurité · **Formation certifiante**

DURÉE	NIVEAU	MODALITÉS	VOUCHER EXAMEN
5 jours	Avancé	Présentiel · Live · Intra	Inclus

Présentation

CompTIA PenTest+ (PT0-003) est une certification avancée qui valide les compétences pratiques du pentesteur : cadrage d'engagement, reconnaissance, exploitation, post-exploitation et reporting. Elle couvre aussi bien les tests d'applications, réseaux, cloud que les scénarios modernes. Elle s'adresse aux professionnels de la sécurité offensive.

Objectifs pédagogiques

- Cadrer et planifier un engagement de test d'intrusion (scope, règles, conformité)
- Conduire la reconnaissance passive et active et l'énumération
- Découvrir, analyser et prioriser les vulnérabilités
- Exploiter des failles réseau, applicatives, sans fil et cloud
- Réaliser la post-exploitation et les mouvements latéraux
- Rédiger des rapports de pentest exploitables et recommander des remédiations

Programme détaillé

1. Module 1 — Gestion de l'engagement

- Cadrage, périmètre et règles d'engagement
- Aspects légaux, conformité et autorisations
- Méthodologies et cadres de pentest
- Communication et gestion des risques

2. Module 2 — Reconnaissance et énumération

- OSINT et reconnaissance passive
- Scans réseau et découverte de services
- Énumération des hôtes, utilisateurs et partages
- Scripting d'automatisation de la reco

3. Module 3 — Découverte et analyse des vulnérabilités

- Scanners de vulnérabilités et analyse des résultats
- Vulnérabilités applicatives et web (OWASP)
- Failles réseau, sans fil et cloud
- Priorisation et validation des findings

4. Module 4 — Attaques et exploitation

- Exploitation réseau et applicative
- Attaques web, injection et déni de service
- Ingénierie sociale et attaques physiques
- Exploitation cloud et conteneurs

5. Module 5 — Post-exploitation et reporting

- Persistance, escalade de privilèges et pivoting
- Mouvements latéraux et exfiltration
- Nettoyage et couverture des traces
- Rédaction du rapport et recommandations de remédiation

Prérequis

Maîtriser les fondamentaux réseau et sécurité (équivalent Network+ et Security+) et disposer de 3 à 4 ans d'expérience en sécurité de l'information.

Public visé

Pentesteurs, analystes sécurité offensive, membres d'équipes Red Team, consultants en cybersécurité et analystes vulnérabilités.

Ce qui est inclus

- Support de cours officiel CompTIA
- Labs offensifs et environnements de pentest
- Examens blancs et préparation à la certification
- Voucher d'examen PT0-003
- Attestation de réussite, pauses et déjeuner inclus

Certification

Examen CompTIA PenTest+ PT0-003 : jusqu'à 90 questions (QCM et questions à performance basée sur des labs), 165 minutes, score de réussite 750/900. Passage chez Advancia Training, centre d'examen agréé Pearson VUE.

1 900 DT HT / participant — tarif inter-entreprise · financement CNFCPP possible