MFE-IT

Formation CompTIA PenTest+

Tests d'intrusion avancés — examen officiel inclus

CompTIA PenTest+ (PT0-003)

Référence : SM/PT0-003

Durée : 5 jours • **Volume horaire : 35 h**

Distanciel · Sessions garanties dès 1 inscrit · 60 % de pratique

DESCRIPTION

Cette formation CompTIA PenTest+ : tests d'intrusion avancés et examen officiel inclus vous prépare à concevoir, planifier, exécuter et analyser des tests d'intrusion complets sur des systèmes, réseaux et applications. Vous apprendrez à utiliser des outils professionnels de pentesting, à effectuer des analyses de vulnérabilités et à documenter vos résultats avec des rapports techniques et exécutifs.

Le programme couvre aussi les cadres légaux et de conformité, la méthodologie offensive et la communication des résultats. Grâce à des ateliers pratiques et des simulations alignées sur les objectifs de l'examen CompTIA PenTest+, vous serez prêt à obtenir une certification reconnue mondialement en cybersécurité offensive.

OBJECTIFS PÉDAGOGIQUES

- Préparer les participants à la certification CompTIA PenTest+ (code PT0-003), reconnue internationalement pour les tests d'intrusion et l'évaluation des vulnérabilités.
- Comprendre les principes fondamentaux des tests d'intrusion, y compris la légalité, la conformité et les cadres réglementaires (RGPD, PCI DSS).
- Acquérir les compétences pour planifier, scoper et exécuter des engagements de tests d'intrusion sur réseaux, systèmes et applications.
- Maîtriser la collecte d'informations, l'analyse de vulnérabilités, les attaques et l'exploitation des failles.
- Savoir documenter et communiquer les résultats de tests, avec des rapports clairs et exploitables pour les équipes techniques et décisionnelles.
- Intégrer des compétences pratiques avancées en cybersécurité pour des environnements hybrides, cloud et applicatifs.

PRÉREQUIS

- Environ 3 à 4 ans d'expérience pratique dans des tests de sécurité, d'intrusion et d'analyse de vulnérabilités.
- Solides connaissances en sécurité informatique, réseaux et systèmes.
- Maîtrise des langages de script (Python, Ruby ou équivalent) recommandée.
- Un entretien préalable avec un expert permet d'adapter le contenu au profil et aux objectifs du participant.

PUBLIC VISÉ

- Pentesters, consultants en sécurité, analystes cybersécurité et ingénieurs sécurité.
- Administrateurs systèmes ou réseaux souhaitant approfondir les tests d'intrusion avancés.
- Professionnels sécurité désirant valider des compétences offensives pratiques via une certification officielle.

PROGRAMME DÉTAILLÉ

Module 1 — Introduction à la certification PenTest+

Objectifs de la certification, environnements légaux, cadres réglementaires.

Module 2 — Planification et scoping

Définir le périmètre des tests, contraintes légales et exigences clients.

Module 3 — Collecte d'informations et analyse de vulnérabilités

Techniques OSINT, reconnaissance réseau et applicative.

Module 4 — Exploitation et attaques

Attaques réseau (ARP spoofing, VLAN hopping), applicatives (XSS, SQLi), mobiles et IoT.

Module 5 — Post-exploitation et mouvements latéraux

Persistance, escalade de privilèges, pivot, couverture des traces.

Module 6 — Reporting et communication

Rédiger et présenter des rapports exploitables pour les équipes techniques et business.

Module 7 — Outils et techniques de pentesting

Usage avancé de Nmap, Nessus, Metasploit, Burp Suite, SQLmap, Wireshark, etc.

Module 8 — Préparation à l'examen CompTIA PenTest+

Exercices pratiques, simulations, QCM et scénarios « performance-based ».

MODALITÉS PÉDAGOGIQUES

Format et déroulement

MFE-IT privilégie un format en mini-groupe (1 à 3 participants), garanti dès un seul inscrit (sauf cas de force majeure). La formation se déroule en distanciel (classe virtuelle synchrone, sessions également enregistrées) ou en présentiel dans vos locaux. Le programme alterne apports théoriques, ateliers pratiques offensifs et simulations d'examen.

Format ultra-personnalisé

Un entretien préalable est organisé avec le participant et/ou un représentant de l'entreprise afin d'adapter le contenu à son niveau, à ses besoins et à ses enjeux professionnels.

Moyens techniques

Un support pédagogique complet est remis à chaque participant. Les sessions s'appuient sur des labs offensifs (Nmap, Metasploit, Burp Suite, etc.), des QCM et des simulations d'examen. Une connexion internet et un poste de travail sont requis pour les sessions à distance.

Évaluation des acquis

Tout au long de la formation, le formateur évalue la progression des participants au moyen de quiz, de mises en situation et de simulations d'examen. Une attestation de fin de formation est remise à l'issue du parcours.

Accessibilité et handicap

Nos formations peuvent être adaptées aux personnes en situation de handicap. Merci de nous contacter en amont afin d'étudier ensemble les modalités d'accueil et d'aménagement (référent handicap : contact@mfe-it.com).

Assistance post-formation

Chaque participant bénéficie d'un accompagnement de 30 jours après la formation pour toute question relative au contenu abordé.

INFORMATIONS PRATIQUES

Prise en compte du handicap

MFE-IT s'engage à étudier toute demande d'aménagement. Un échange avec notre référent handicap permet d'adapter les conditions d'accueil et de déroulement de la formation.

Modalités pédagogiques et techniques

Formation en distanciel (classe virtuelle synchrone) ou en présentiel dans vos locaux, en mini-groupe. Alternance de théorie, d'ateliers pratiques offensifs et de simulations d'examen.

Moyens du formateur

Formateur expert certifié, support de cours complet, labs offensifs et simulations d'examen.

Validation et sanction

Attestation de fin de formation. Cette formation inclut le passage de l'examen officiel CompTIA PenTest+ (PT0-003).

Type de formation

Action de formation professionnelle continue : acquisition et perfectionnement de compétences.

Suivi de l'exécution

Feuilles de présence signées, évaluations en cours de formation et attestation de fin de formation.

Modalités d'évaluation

Quiz, mises en situation, QCM et simulations d'examen tout au long de la formation.

Aide à l'orientation

La CompTIA PenTest+ complète le volet offensif du parcours cybersécurité (après CompTIA Security+ et CySA+).