CompTIA Penetration Testing (PENTEST+)

Description

Maîtrisez les tests de pénétration avec la certification CompTIA Penetration Testing (PENTEST+)

La formation CompTIA Penetration Testing (PENTEST+) est idéale pour les professionnels de la cybersécurité souhaitant approfondir leurs compétences en tests de pénétration. Dans ce programme intensif, vous apprendrez à planifier, exécuter et analyser des tests complets pour identifier les vulnérabilités des systèmes. Que vous soyez pentester, analyste ou opérateur, cette certification vous aidera à démontrer votre expertise dans un domaine en constante évolution. Avec l'augmentation des cybermenaces, cette formation offre des compétences précieuses pour sécuriser les réseaux et les applications des entreprises.

En plus d'une préparation complète à l'examen PT0-002, vous acquerrez des compétences pratiques à travers des laboratoires virtuels et des exercices en conditions réelles. Vous apprendrez à utiliser des outils et des scripts pour collecter, analyser et exploiter des données dans divers environnements réseau. Cette formation vous permet de devenir un atout indispensable pour toute équipe de sécurité, en maîtrisant l'ensemble du processus de test de pénétration, du plan à l'élaboration de rapports complets.

Contenu du cours
Module 1 : Planifier et définir le périmètre des tests de pénétration

- Présentation des méthodes de test de pénétration
- Planification d'une opération de PenTest
- Évaluation et négociation d'une prestation de PenTest
- Préparation à la réalisation des tests de pénétration

Module 2 : Procéder à une exploration passive

- Collecte des données générales
- Préparation des données de base requises pour les actions à venir

Module 3 : Effectuer des tests de pénétration

- Réalisation de tests d'ingénierie sociale
- Réalisation de tests de sécurité physique relatifs aux infrastructures

Module 4 : Procéder à une exploration active

- Numérisation des réseaux
- Identification des sources de données
- Détection des risques de vulnérabilité
- Analyse avec des scripts de base

Module 5 : Analyser les facteurs de vulnérabilité

- Analyse des résultats de la détection des vulnérabilités
- Extraction des données pour la préparation des tests réseau

Module 6 : Pénétrer les réseaux de communication

- Exploitation des vulnérabilités du réseau câblé, du réseau sans fil et des systèmes de radio fréquences
- Exploitation des vulnérabilités des réseaux spécifiques

Module 7 : Analyser les vulnérabilités basées sur l'hôte

- Analyse des vulnérabilités du système d'exploitation Windows
- Analyse des vulnérabilités du système d'exploitation Linux

Module 8 : Tester les logiciels et les applications

- Exploitation des vulnérabilités pour les apps Web
- Test du code source des logiciels et des applications (compilation incluse)

Module 9 : Achever les activités de post-exploitation

- Utilisation des techniques de déplacement latéral
- Utilisation des techniques de rémanence
- Utilisation des techniques anti-médico-légales

Module 10 : Rédiger un rapport de tests de pénétration

- Analyse des résultats des tests de pénétration
- Élaboration de recommandations de stratégies d'atténuation
- Rédaction et gestion d’un rapport
- Réalisation des tâches post-rapport

Documentation

- Support de cours numérique inclus

Examen

- Ce cours prépare à la certification CompTIA PenTest+.
- Pour obtenir la certification CompTIA PenTest+, les candidats doivent réussir l'examen : PT0-002.
- Si vous souhaitez passer ces examens, veuillez contacter notre secrétariat qui vous informera du coût des examens et prendra en charge toutes les démarches administratives nécessaires pour vous.

Profils des participants

- Pentesters
- Analystes en cybersécurité
- Testeurs de vulnérabilités
- Responsables de la sécurité des systèmes d'information
- Consultants en sécurité

Connaissances Préalables

- Maîtrise des concepts de réseau et de sécurité
- Expérience avec des outils de pentest comme Metasploit
- Connaissances des systèmes d'exploitation (Windows, Linux)
- Capacité à utiliser des scripts Bash, Python, Ruby ou PowerShell
- Compréhension des protocoles réseau (TCP/IP, DNS, HTTP)

Objectifs

- Planifier et organiser des tests de pénétration
- Exploiter les vulnérabilités des réseaux câblés et sans fil
- Collecter et analyser des données pour détecter des failles
- Utiliser des scripts pour automatiser les tests
- Analyser les vulnérabilités des systèmes et des applications
- Élaborer et rédiger des rapports de tests de pénétration

Description
Formation CompTIA Penetration Testing (PENTEST+)
Niveau
Intermédiaire
Prix de l'inscription en Présentiel (CHF)
4000
Prix de l'inscription en Virtuel (CHF)
3750
Durée (Nombre de Jours)
5
Reference
COM-202