Certified Penetration Testing Professional (CPENT)

Description

Qu’est-ce que la certification Certified Penetration Testing Professional (CPENT) ?

Certified Penetration Testing Professional (CPENT) est une formation complète et avancée dédiée aux professionnels de la cybersécurité qui souhaitent maîtriser les techniques de tests d’intrusion. Reconnu dans le domaine, ce programme vous permet d’acquérir des compétences approfondies pour analyser et pénétrer des réseaux complexes, tout en exploitant les vulnérabilités existantes. La certification CPENT couvre un large éventail de sujets, allant des tests d’intrusion sur les réseaux, l’IoT et les technologies OT/SCADA, jusqu’à l’exploitation des systèmes cloud et la rédaction de rapports professionnels.

Pourquoi choisir la formation CPENT ?

Cette formation se distingue par son approche pratique et réaliste, avec des laboratoires dynamiques qui évoluent pour simuler les menaces actuelles. En suivant le programme Certified Penetration Testing Professional (CPENT), vous vous assurez de maîtriser non seulement les techniques d’intrusion, mais aussi la rédaction de rapports exploitables pour les parties prenantes. La formation vous permet de personnaliser des scripts, d’optimiser les tests en double pivot et de gérer efficacement les environnements sécurisés. C’est l’opportunité de développer des compétences essentielles pour sécuriser des infrastructures variées, de l’IoT au cloud.

Reference
CPENT
Contenu du cours
Module 1 : Introduction to Penetration Testing

- Fondamentaux des tests d'intrusion
- Éthique et cadre légal

Module 2 : Penetration Testing Scoping and Engagement

- Établissement des objectifs
- Définition des périmètres d’intervention

Module 3 : Open-Source Intelligence (OSINT)

- Recherche d’informations via des sources publiques
- Utilisation d’outils OSINT

Module 4 : Social Engineering Penetration Testing

- Manipulation humaine pour accéder à des données sensibles
- Techniques de phishing et vishing

Module 5 : Network Penetration Testing – External

- Tests sur les infrastructures externes
- Exploitation des failles de sécurité

Module 6 : Network Penetration Testing– Internal

- Audit des réseaux internes
- Exploitation des services réseaux compromis

Module 7 : Network Penetration Testing – Perimeter Devices

- Tests sur les dispositifs de sécurité (pare-feu, routeurs)
- Évaluation des configurations de sécurité

Module 8 : Web Application Penetration Testing

- Tests d'intrusion sur les applications web
- Exploitation des vulnérabilités des applications

Module 9 : Wireless Penetration Testing

- Audit des réseaux sans fil
- Exploitation des failles dans les réseaux Wi-Fi

Module 10 : IoT Penetration Testing

- Analyse des dispositifs IoT
- Exploitation des failles dans les systèmes connectés

Module 11 : OT/SCADA Penetration Testing

- Tests sur les systèmes industriels
- Évaluation des vulnérabilités dans les environnements OT

Module 12 : Cloud Penetration Testing

- Audit des environnements cloud
- Exploitation des configurations incorrectes

Module 13 : Binary Analysis and Exploitation

- Analyse des fichiers binaires
- Exploitation des vulnérabilités logicielles

Module 14 : Active Directory Penetration Testing

- Tests d'intrusion sur les environnements Active Directory
- Exploitation des failles AD

Module 15 : Report Writing and Post Testing Actions

- Rédaction de rapports d'audit
- Actions post-test

Documentation

- Support de cours numérique inclus

Examen

- Ce cours prépare à la certification Certified Penetration Testing Professional (CPENT).
- Pour obtenir la certification Certified Penetration Testing Professional (CPENT), les candidats doivent réussir l'examen
- Si vous souhaitez passer cet examen, 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

- Consultants en sécurité
- Administrateurs systèmes et réseaux
- Professionnels en tests d'intrusion
- Experts en cybersécurité
- Architectes de solutions de sécurité

Connaissances Préalables

- Bonne maîtrise des fondamentaux en cybersécurité
- Connaissance des systèmes d'exploitation Windows et Linux
- Compétences de base en scripts et automatisation
- Expérience préalable en tests d'intrusion
- Compréhension des réseaux et des protocoles TCP/IP

Objectifs

- Maîtriser les attaques avancées sur Windows
- Réaliser des tests d'intrusion sur les systèmes IoT
- Exploiter des binaires : exploitation avancée
- Contourner les réseaux filtrés
- Tester les systèmes OT/SCADA
- Accéder à des réseaux cachés avec pivoting

Description
Formation Certified Penetration Testing Professional (CPENT)
Niveau
Intermédiaire
Prix de l'inscription en Présentiel (CHF)
5900
Prix de l'inscription en Virtuel (CHF)
5650
Durée (Nombre de Jours)

5