Organisme de formation professionnelle continue
Numero agrément 91 30 03332 30
France : +33 (0)188 24 70 33 / 34
Site : www.oo2.fr
Mail : contact@oo2.fr

CompTIA PenTest+ : tests de pénétration et gestion des vulnérabilités

Date et durée

Code formation : C-PEN
Durée : 5 jours
Nombre d'heures : 35 heures

Formation avec certification

CompTIA PenTest+

Description

CompTIA PenTest+ est une formation certifiante dédiée aux spécialistes de la cybersécurité qui sont responsables des tests de pénétration et de la gestion des vulnérabilités. Que vous soyez **pentester, analyste ou opérateur en cybersécurité**, elle vous permet de prouver que votre niveau de connaissances est plus élevé que celui d'un débutant et vous donne les moyens d'apporter une valeur ajoutée à une équipe de pentest.
Comme les entreprises luttent contre les cybermenaces pour protéger leurs business et leurs clients, savoir **mener des tests de pénétration** est une nouvelle compétence qui devient de plus en plus prisée. Dans ce programme, vous apprendrez à maîtriser les méthodologies et les principes fondamentaux des tests de pénétration. Vous aborderez le côté **gestion des vulnérabilités** et vous serez amené à exécuter un test de pénétration pour appliquer la partie théorique de ces cours. Pour conclure, vous traiterez de la **mise en œuvre de rapports de test** et des tâches post-rapport.
Au terme de cette formation de 5 jours, vous serez également **préparé pour le passage de l'examen CompTIA PT0-002** inclus dans notre offre. Cet examen est un prérequis pour obtenir la certification CompTIA PenTest+ (*en savoir plus dans l'onglet certification*).

Objectifs

À l'issue de la **formation CompTIA PenTest +**, vous atteindrez les objectifs de compétences suivants :

- comprendre la nécessité de planifier et connaître les principaux avantages des tests de conformité ;
- collecter des données pour le traitement de l'exploitation et réaliser une analyse de vulnérabilité afin d'effectuer une analyse des résultats ;
- exploiter des vulnérabilités dans les connexions réseaux câblées et sans fil, dans les logiciels, applications et dans les systèmes de radio fréquence ;
- synthétiser des attaques de sécurité physique et employer des techniques de post exploitation ;
- réaliser des opérations de collecte de données en utilisant divers outils et effectuer une analyse des résultats en utilisant des scripts de base avec Bash, Python, Ruby ou encore PowerShell ;
- se servir des bons outils de conception et de gestion de rapports afin d'expliquer et de recommander des stratégies visant à limiter les failles de sécurité qui ont été identifiées ;
- passer l'examen PT0-002 PenTest+ et décrocher la certification.

La certification CompTIA PenTest+ est renouvelable en cumulant 60 unités de formation continue (CEU) sur 3 ans.
En savoir + sur le programme de formation continue CompTIA

Points forts

10 cours pour acquérir ou valider des compétences en tant que Pentester ; une formation qui traite des tests de pénétration les plus récents et le passage de l'examen de certification CompTIA PenTest+ compris dans l'offre.

Certification

Notre formation CompTIA PenTest+ vous permettra de **passer l'examen officiel CompTIA PT0-002** à tout moment et en ligne. Pour planifier votre examen, vous devez vous inscrire sur CompTIA.org. Après avoir réussi cet épreuve, vous obtiendrez la **certification CompTIA PenTest+ valable 3 ans**.

Détail de l'examen CompTIA PT0-002 :

L'examen certifie que vous possédez les connaissances et les compétences indispensables à la planification et à la conception d'une analyse, à la bonne appréciation des normes juridiques et de la règlementation, à **la conduite de tests de vulnérabilité et de tests de pénétration**, à l'analyse des données, et enfin à la rédaction de rapports sur les résultats.

- Type d’examen : 85 questions à choix multiples et basés sur la performance
- Durée : 2 h 45
- Livre ouvert : non
- Langues : anglais, japonais, portugais et thaï
- Attribution : 750 points basés sur une échelle de 900 points

Modalités d'évaluation

Quiz / QCM
Travaux Pratiques

Pré-requis

Suivre la **formation CompTIA PenTest+** nécessite les prérequis suivants :

- avoir une expérience pratique de 3 ans minimum dans le domaine de la sécurité de l'information ou toute autre expérience annexe ;
- savoir lire et comprendre l'anglais, le japonais ou le thaï pour le passage de l’examen PT0-002.

Formations recommandées :

Les formations ci-dessous sont recommandées.

CompTIA S+ : les bases de la cybersécurité
CompTIA N+ : configuration, gestion et dépannage des réseaux

Public

Cette formation s'adresse aux publics suivants :

- les professionnels de la cybersécurité responsables des tests de pénétration et de la gestion des failles de sécurité ;
- les testeurs de vulnérabilités, testeurs de pénétration ou les analystes de sécurité qui souhaitent obtenir la certification CompTIA PenTest+.

Cette formation s'adresse aux profils suivants

Pentester (tests d'intrusion)
Analyste cybersécurité

Programme

Cours 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.

Cours 2 : procéder à une exploration passive

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

Cours 3 : effectuer des tests de pénétration

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

Cours 4 : procéder à une exploration active

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

Cours 5 : analyser les facteurs de vulnérabilité

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

Cours 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.

Cours 7 : analyser les vulnérabilités basées sur l'hôte

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

Cours 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).

Cours 9 : achever les activités de post-exploitation

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

Cours 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.

Guide des certifications CompTIA
Télécharger la brochure