CompTIA PenTest+

Objectifs

- 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.

Prérequis

- 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.

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.