Certification Certified Ethical Hacker (CEH)

Objectifs

Au cours de ce cours, vous devrez apprendre :

- Les problèmes clés incluent le monde de la sécurité de l'information, le piratage éthique, les contrôles, les lois et les normes de sécurité de l'information.
- Effectuez une empreinte et une reconnaissance à l'aide des dernières techniques d'empreinte, notamment l'empreinte via les services Web et les sites et outils de réseaux sociaux, en tant que phase préalable à l'attaque critique requise dans le piratage éthique.
- Techniques d'analyse réseau et contre-mesures d'analyse.
- Techniques de dénombrement et contre-mesures de dénombrement.
- Analyse des vulnérabilités pour identifier les failles de sécurité dans le réseau, l'infrastructure de communication et les systèmes finaux de l'organisation cible.
- Méthodologie de piratage du système, stéganographie, attaques par stéganalyse et couverture des pistes pour découvrir les vulnérabilités du système et du réseau.
- Différents types de menaces de logiciels malveillants (chevaux de Troie, virus, vers, etc.), audit du système pour les attaques de logiciels malveillants, analyse des logiciels malveillants et contre-mesures.
- Techniques de reniflage de paquets pour découvrir les vulnérabilités du réseau et contre-mesures pour défendre le reniflage.

Prérequis

- Avoir deux ans d'expérience en sécurité informatique et posséder une connaissance de base de Linux et/ou Unix.
- Familiarité avec les concepts de cybersécurité
- Une solide connaissance pratique de : TCP/IP, Windows Server

Programme

Appliquer les concepts procéduraux nécessaires pour identifier les attaquants grâce à la modélisation des menaces

- Interpréter les données entrantes et sortantes pour déterminer l'utilisation autorisée et non autorisée
- Appliquer les concepts procéduraux nécessaires pour identifier les vulnérabilités dans les systèmes d'information
- Appliquer les concepts procéduraux nécessaires pour effectuer des évaluations des risques pour les réseaux et les systèmes basés sur l'information
- Dans un scénario, déterminer les méthodes de chiffrement et de déchiffrement appropriées
- Appliquer le contre-traitement procédural des concepts nécessaires pour trouver et contenir les logiciels malveillants et les virus

Interpréter les lois et réglementations en vigueur pour fournir des mises à jour des politiques de sécurité organisationnelles

- Dans un scénario, déterminer la méthode appropriée pour aider au développement de nouveaux logiciels et aux tests de l'utilisateur final
- Dépanner divers produits et systèmes de sécurité pour valider leur fonction

Compte tenu d'un scénario, déterminer la méthode appropriée pour mettre en œuvre les protocoles de sécurité et la gestion pour les systèmes d'exploitation courants

- Dans un scénario, déterminer comment se défendre contre différents types d'attaques
- Appliquer les concepts procéduraux nécessaires pour configurer les systèmes de sécurité et valider la sécurité

Déterminer la méthode appropriée pour effectuer des tests d'intrusion afin d'évaluer les faiblesses et les vulnérabilités

- Compte tenu d'un scenario, analyser les atteintes à la sécurité des réseaux
- Appliquer les concepts procéduraux nécessaires pour mener différents types d'ingénierie sociale

Appliquer les concepts procéduraux nécessaires pour identifier différentes méthodes d'identification, d'authentification et d'autorisation

- Appliquer les concepts procéduraux nécessaires pour identifier l'emplacement approprié des dispositifs biométriques

Identifier différents types de cryptographie

- Compte tenu d'un scénario, déterminer le cryptographe approprié