

Formation sécurité informatique: Piratage avancé et détection d'intrusion

(AHAIDFR, 4 jours)

Description

Le cours Formation sécurité informatique : Piratage avancé et détection d'intrusion explore le piratage avancé dans une perspective de sécurité offensive. Le cours couvre le piratage avec Metasploit et aborde les techniques d'attaque courantes, notamment l'injection SQL, les scripts intersites, le phishing, l'usurpation d'identité et plus encore. La formation aborde également la planification et la mise en œuvre d'un système de détection d'intrusion ainsi que la conception et la mise en œuvre de processus de sécurité informatique connexes, notamment la gestion des incidents, des problèmes, des événements et de la sécurité informatique.

Tarifs

- Tarification: \$3,750/person
- Rabais de 10% lorsque vous inscrivez 3 personnes.

Plan de cours

Le cycle de vie du piratage

Le rôle essentiel de l'ingénierie sociale

Utilisation de Metasploit : Révision et consolidation

Outils et techniques de collecte d'informations

Analyse de l'environnement cible

Réalisation d'une évaluation de la vulnérabilité

Utiliser Metasploit pour s'imposer

Escalade de vos privilèges

Maintien de l'accès

Piratage de services communs

Techniques de piratage avancées

Utilisation du phishing et d'autres stratégies de courrier électronique

Réalisation d'une évaluation de la vulnérabilité d'un site ou d'un service Web

Utilisation du courrier électronique et de serveurs Web temporaires pour obtenir un accès

Attaquer les applications et services Web à l'aide de l'injection SQL

Attaque des applications et services Web à l'aide de Cross-Site Scripting

Protéger vos actifs Web

Prévention des attaques par injection SQL

Protection contre les attaques XSS

Verrouillage des services et applications Web par la suppression des en-têtes

Utilisation de SSL et HTTPS

Utilisation de l'authentification et de l'autorisation dans les actifs Web

Désactiver les codes faibles

Déploiement des assemblages et définition de la configuration

Détection d'intrusion

Le rôle de la détection des intrusions par rapport à l'authentification et à l'autorisation.

Ce que la détection d'intrusion peut et ne peut pas fournir

Les types de détection d'intrusion : NIDS, NNIDS et HIDS

Où les IDS devraient être positionnés

Le rôle essentiel des processus

Processus de gestion des incidents, des problèmes et des événements

Mise en œuvre d'un IDS

Aperçu de l'oignon de la sécurité

Mise en œuvre des alertes

Travailler avec des données d'actifs

Captures de paquets et données de contenu intégral

Capturer et travailler avec les données de l'hôte

Capturer et travailler avec les données de session

Capturer et travailler avec les données de transaction

Étude de cas de mise en œuvre : Détection des intrusions dans les services Web