SETC Training Corporate Logo

Formation sécurité informatique: Essentiels de la cybersécurité (CYSECEFR, 4 jours)

Description

Le cours Formation sécurité informatique : Essentiels de la cybersécurité est une exploration du cycle de vie complet de la sécurité informatique des entreprises. La formation commence par un examen des concepts clés des réseaux, notamment l'adressage IP, les commutateurs, les routeurs, les VLAN, la VOIP, et se termine par une étude complète des concepts de cybersécurité tels que l'assurance de l'information, la cryptographie, l'authentification et les considérations juridiques et réglementaires. Le cours s'appuie ensuite sur ces concepts fondamentaux pour explorer les aspects pratiques de la sécurisation des routeurs, des commutateurs et des ordinateurs fonctionnant sous Windows et Linux. La formation couvre également les systèmes de détection d'intrusion (IDS) et les politiques et procédures essentielles qui soutiennent la sécurité informatique dans une organisation. Le cours se termine par une étude détaillée des attaques de pirates, notamment les méthodes d'attaque, le vecteur d'attaque, le traitement des incidents et les techniques d'atténuation.

Tarifs

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

Plan de cours

Principes fondamentaux des réseaux

- Le modèle de référence OSI et la structure des paquets
- Concepts IP essentiels : Adresses IP et sous-réseaux
- Obtention d'une adresse IP : Adressage statique et dynamique
- Concepts IP essentiels : Protocoles de transport (TCP et UDP)
- Comportement IP : Comprendre les sockets, les ports et les protocoles d'application
- Comprendre les routeurs et les commutateurs de couche 3
- Travailler avec et comprendre les VLAN
- Explorer les technologies VOIP

Sécurité informatique : Concepts essentiels

- Fondements de l'assurance de l'information
- Cryptographie et communications sécurisées
- Sécurité des programmes : Failles et défenses
- Sécurité du système d'exploitation
- Identification et authentification
- Systèmes d'exploitation et systèmes de gestion de bases de données fiables
- Sécurité des réseaux : Menaces, contrôles et technologies
- Gestion de la sécurité
- Questions juridiques, de confidentialité et d'éthique

Mise en œuvre de la sécurité des routeurs

- Pare-feu : Rôles et concepts
- Cisco IOS : Le rôle des filtres de routeur, de la QoS et de la NAT
- Cisco IOS : Implémentation des classes et des cartes de classe
- Cisco IOS : Implémentation des ACLs
- Cisco IOS : Mise en œuvre des politiques

Sécurisation de l'ordinateur : Windows

- Explorer les orientations du NIST en matière de cybersécurité
- Création d'une politique de sécurité de l'information

Créer des utilisateurs et gérer les permissions sous Windows
Appliquer la complexité et le vieillissement des mots de passe
Gestion des administrateurs de domaine et du compte administrateur
Gestion des permissions : Système de fichiers Windows et sécurité des partages
Créer une politique de groupe et renforcer la sécurité du domaine
Sécurisation de la base de données SAM

Sécuriser l'ordinateur : Linux

Créer des utilisateurs et gérer les permissions sous Linux
Utilisation des modules PAM pour renforcer la complexité et l'âge des mots de passe
Gestion de l'accès aux racines
Limiter les connexions à distance
Sécuriser SSH
Gestion des permissions : Système de fichiers Linux et sécurité basée sur le partage
Sécurisation des fichiers clés de sécurité
Mise en œuvre de SELinux (facultatif)

Mise en œuvre de la sécurité des ordinateurs

Comprendre les vulnérabilités informatiques
Mise en œuvre de la journalisation et de l'audit sur un ordinateur
Désactivation du matériel vulnérable
Désactivation des services non essentiels
Conception et mise en œuvre d'une stratégie de mise à jour des logiciels
Validation de l'intégrité d'une mise à jour

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

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

Politiques et procédures

Aperçu des processus clés
Explorer la gestion de la sécurité de l'information
Exploration de la gestion de la continuité des activités
Le processus de gestion des risques de A à Z
Identification des risques : Création du registre des risques
Évaluation des risques : Déterminer la probabilité et l'impact
Réalisation d'une analyse de SPOA et d'une analyse d'impact sur les affaires
Gestion des risques : Planification de l'atténuation
Audits de risques : Principes et application
Rédaction d'un plan de communication
Mise à jour du plan de continuité des services informatiques et du plan de continuité des activités
Conception d'une gestion efficace des incidents

Assurer la gestion des problèmes
Le rôle de la gestion du changement et de la gestion du changement d'urgence
L'importance de la gestion de la configuration des actifs de services

Explorer les méthodes d'attaque

Comprendre l'état d'esprit du hacker
Explorer les méthodes d'attaque
Les 10 principales vulnérabilités en matière de sécurité
Exploration du détournement de session
Explorer l'homme du milieu
Explorer l'injection SQL
Exploration de XSS
Explorer l'exposition des données sensibles
Explorer l'authentification brisée
Explorer les failles du WIFI et les protocoles de sécurité
Une note sur les ransomwares
La place du déni de service (DOS)
Techniques de gestion des menaces persistantes avancées

Autres concepts utiles

Guerre de l'information offensive et défensive
Mise en œuvre des pots de miel
Mise en œuvre des Service Packs d'OS et de logiciels
Empêcher l'utilisation de dispositifs non autorisés
Formation des utilisateurs
Assurer des tests de sécurité réguliers
Utilisation d'algorithmes cryptographiques appropriés
Exploration de la sténographie et des formats de fichiers connus

Le vecteur d'attaque

La phase de définition de l'objectif
La phase de collecte d'informations
À propos de Target Discovery
Énumération de la cible
Cartographie des vulnérabilités
Ingénierie sociale
Exploitation des cibles
Escalade de privilèges
Tout mettre en place

Traitement des incidents

La pratique rend parfait : Former le personnel à réagir à une situation d'attaque
Comment savoir si vous êtes attaqué
Avant de commencer : Identifier la cause profonde
Identifier et exécuter la réponse
Limiter l'étendue des dommages
Examen des journaux et identification des systèmes compromis
Communiquer avec les personnes affectées
Prévenir les attaques futures
Effectuer une autopsie