SETC Training Corporate Logo

Formation Cisco: Maîtriser la sécurité des réseaux (CSCADVFR, 4 jours)

Description

Le cours Formation Cisco : Maîtriser la sécurité des réseaux se penche sur les détails de la sécurité des réseaux Cisco. Chaque aspect de la mise en œuvre de la politique de sécurité est couvert, depuis les considérations de base sur les protocoles jusqu'à l'utilisation des pare-feu, IPS et IPv6. La formation inclut les ACLs, les protocoles de tunneling et de routage.

Tarifs

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

Plan de cours

Principes fondamentaux de la sécurité

- Introduction à la sécurité des réseaux
- La nécessité de la sécurité des réseaux
- Options de sécurité du réseau
- Pourquoi les pirates informatiques piratent-ils ?
- Objectifs généraux de la sécurité des réseaux
- Attaques d'ingénierie sociale et d'escalade de privilèges
- Comprendre les balayages Ping et l'audit réseau de base

Introduction au SDM (Security Device Manager)

- Security Device Manager (SDM) de Cisco
- Configuration de la pré-installation
- Installation, lancement et chargement de SDM
- Paramètres et configuration du SDM
- Surveillance SDM

Authentification, autorisation et comptabilité (AAA)

- Aperçu de "Qu'est-ce que l'AAA ?"
- TACAS+ vs. Radius
- Configuration de TACAS+ et Radius
- Aperçu des principes d'authentification
- Comptabilité
- Autorisation
- Configuration de l'AAA avec SDM

Sécurité de la couche 2

- Fonctions de base de la sécurité L2
- Aperçu de la sécurité des ports
- Configurer ou mal configurer la sécurité du port
- L'heure du vieillissement pour l'accès sécurisé et les adresses collantes
- Protocole d'authentification extensible légère de Cisco (LEAP)
- Configuration du SPAN local et distant
- Filtrage du trafic intra-VLAN
- Liste d'accès aux VLAN (VACL)
- VLAN privé
- DHCP Snooping et inspection ARP dynamique

IP Source Guard
Attaques par inondation d'adresses MAC et saut de VLAN
Garde racine et BPDU

Sécurité de la couche 3

Configuration et chiffrement des mots de passe dans Cisco IOS
Niveaux privilégiés
Créer et tester la politique de longueur minimale des mots de passe
Mots de passe forts ou faibles
"Salage" de votre MD5
Protocole de temps réseau (NTP)
Synchronisation et configuration de NTP
Accès à distance Telnet et SSH
Les différents types d'attaques de réseau
Attaque par déni de services (DoS) et inondation SYN
ICMP (Ping) Sweep, Port Scan, et Port Sweep
Attaques et inondations Ping
Usurpation d'identité IP et routage à la source
Renifleurs de paquets et requêtes
Introduction à l'audit de sécurité
Virus et vers
Différences entre SDM et AutoSecure

Le système de prévention des intrusions (IPS)

Détection d'intrusion (IDS) vs. prévention d'intrusion (IPS)
Signatures et types de signature
NIPS et HIPS
Honeypots
Configurer IPS dans SDM
Visualisation et modification des signatures
Vérifier une configuration IPS

Pare-feu

Les bases des pare-feu
Pare-feu avec ou sans état
Passerelle de la couche d'application (ALG)
Les composants du jeu de fonctions du pare-feu Cisco IOS
Proxy d'authentification
Révision des ACL et listes de contrôle d'accès étendues
Introduction aux Turbo ACLs
Inspection générique TCP et UDP
Inspection en profondeur (DPI)
Configuration du pare-feu par zone
Cartes de classe et cartes de politique
Configuration et commandes de base de la zone
Pare-feu avec SDM

Cryptographie et réseaux privés virtuels (VPN)

Introduction aux techniques de cryptographie
Algorithmes asymétriques et symétriques
Aperçu des algorithmes cryptographiques courants
Qu'est-ce qu'un VPN ?
Terminologie et théorie des VPN
Introduction à l'ICP et au certificat d'autorité

Normes de cryptographie à clé publique et échange de clés sur Internet

Critères de correspondance des politiques et ACLs Crypto

Utilisation de SDM pour configurer le VPN site à site

Encapsulation de routage générique (GRE) sur IPSec

Utilisation de SDM pour configurer GRE sur IPSec

Introduction aux solutions réseau Cisco

Cycle de vie du développement du système

Phases du SDLC de Cisco

Techniques de reprise après sinistre

Analyse du risque - Quantitative et Qualitative

Réseau d'autodéfense Cisco

Cisco Security Management Suite

Agent de sécurité et intercepteurs Cisco