



Référence : STC - CISCO - IINS

5 jours - 35h

IINS

NIVEAU UTILISATEUR

Découverte

Initiation

Maîtrise

Expertise

Informations Cours

Durée : 35 heures - 5 jours

Certification préparée : Cisco 640-553

Durée de la certification : xxxxx

Public : Techniciens, Ingénieurs réseaux, Architecte

Pré-requis

- Avoir suivi les formations ICND1 et ICND2

Contenu de la formation

Introduction aux principes de sécurité réseau

- Les fondamentaux de la sécurité réseau
- Étude des méthodologies d'attaque
- Opérations de sécurité
- Comprendre et développer une politique de sécurité pertinente
- Construire le Cisco Self-Defending Network

Périmètre de sécurité

- Sécuriser l'accès administratif aux routeurs Cisco
- Introduction au Cisco Security Device Manager (SDM)
- Configuration du AAA avec base locale sur un routeur
- Configuration du AAA avec l'Access Control Server (ACS) sur un routeur
- Implémentation du reporting et du management sécurisé
- Blinder le routeur Cisco

Cisco IOS Firewall

- Introduction aux technologies firewall
- Création de filtres grâce aux Access Control Server (ACL)
- Configurer le firewall en mode Zone-Based

VPN Site à Site

- Introduction aux services cryptographiques
- Explication du chiffrement symétrique
- Explication des signatures digitales et des fonctions de hachage
- Explication du chiffrement asymétrique et des PKI
- Fondamentaux IPsec
- Construire un tunnel IPsec Site à site en CLI
- Construire un tunnel IPsec Site à site via le SDM

Cisco IPS

- Introduction aux technologies IPS
- Configuration de l'IPS via le SDM

LAN, SAN, Voix et sécurisation du poste utilisateur

- Explication de la sécurité du poste utilisateur
- Explication de la sécurité du SAN
- Explication de la sécurité de la voix
- Réduction des attaques niveau

Travaux Pratiques

- Insertion de mot de passe avec la stéganographie
- Scan d'un poste client
- Scan d'un réseau
- Sécurisation de l'accès administratif d'un routeur
- Configuration du AAA via la base locale du routeur
- Configuration du AAA via le serveur ACS sur un routeur
- Implémentation du reporting et du management sécurisé
- Utilisation des outils SDM : One-Step Lockdown et Security Audit
- Configuration du filtrage via les ACLs
- Configuration du firewall en mode Zone-based
- Configuration d'un tunnel VPN Site à Site
- Configuration du Cisco IPS
- Fonctionnalités de sécurité sur les switches

Compétences acquises/Objectifs

- Comprendre et implémenter des politiques de sécurité pour contrecarrer les menaces sur le système d'information
- Configurer les routeurs de périphérie grâce aux fonctionnalités de sécurité intégrées au Cisco IOS
- Configurer les différents éléments des firewalls incluant les Access Control List (ACL) et le firewalling en zone
- Configurer un VPN IPsec site à site
- Activer et configurer l'Intrusion Prevention System (IPS) intégré dans le Cisco IOS
- Paramétrer les équipements niveau 2 pour le contrôle d'accès et stopper les attaques orientées LAN