IMPLEMENTING CISCO NETWORK SECURITY

Cette formation permet aux participants d'acquérir les compétences et connaissances nécessaires pour concevoir, mettre en œuvre et surveiller les stratégies de sécurité, via les fonctionnalités et technologies de sécurité Cisco IOS.
Tous les exemples d'IOS et l'expérience pratique sont acquis via IOS CLI. IPS est abordé de façon théorique via les produits FirePower. La configuration VPN site à site est couverte à la fois sur Cisco IOS et sur les Cisco ASA. Des exemples de Malware récents et des techniques de cryptographie utilisant le hashing et des algorithmes de cryptage sont abordés. Les versions récentes des IOS, Cisco ASA et Cisco Anyconnect seront utilisés.

CODE DE LA FORMATION:
CS-SC-IINS

ÉDITEUR OU CONSTRUCTEUR:
CISCO

VERSION:
3.0

DURÉE:
5 JOURS

PRÉREQUIS:
Avoir suivi les cours ICND1 ou posséder les connaissances équivalentes.

PUBLIC:
Cette formation s'adresse aux personnes désirant acquérir et comprendre la sécurité des réseaux Cisco.

OBJECTIFS:
- Décrir les menaces courantes
- Sécuriser la gestion et le plan de contrôle des périphériques réseaux
- Décrire les technologies de défense contre les menaces
- Sécuriser la gestion et le plan de contrôle des périphériques réseaux
- Configurer AAA sur les périphériques IOS Cisco
- Mettre en œuvre la gestion sécurisée pour les Cisco ASA et les routeurs et switchs Cisco IOS
- Sécuriser le plan de contrôle
- Sécuriser la gestion et les plans de contrôle des périphériques réseaux
- Mettre en œuvre la sécurité de l'infrastructure de la couche 2
- Mettre en œuvre la sécurité des protocoles de la couche 2
- Configurer la gestion des accès et du NAT sur les Cisco ASA
- Configurer le contrôle d'accès et les stratégies de service sur les Cisco ASA
- Décrire IPSec
- Mise en place d'un accès client VPN-distant
- Mettre en œuvre un accès distant VPN sans client
- Décrire IPS et IDS
- Décrire la protection des postes de travail
- Décrire la sécurité sur l'analyse des contenus
- Décrire les architectures de sécurité réseau

CONTENU:

Concepts de sécurité

- Les différents types d'attaques
- Technologies de défense contre les menaces
- Stratégie de sécurité et architectures de sécurité de base
- Technologies de cryptographie

Périphériques réseau sécurisés

- Mettre en œuvre AAA
- Les protocoles de management et systèmes
- Sécuriser le plan de contrôle

Sécurité de la couche 2

- Infrastructure sécurisée de la couche 2
- Sécuriser les protocoles de la couche 2

Firewall

- Technologies FirewallIntroduction à Cisco ASA v9.2
- Introduction à Cisco ASA v9.2
- Contrôle d'accès Cisco ASA et stratégies de service
- Firewall sur Cisco IOS

VPN

- Technologies IPSec
- VPN site à siteAccès VPN distant basé sur le client
- Accès VPN distant basé sur le client
- Accès distant VPN sans client

Sujets avancés

- Détection des intrusions et Protection
- Protection des Postes de travail
- Sécurité sur l'analyse du contenu
- Architectures avancées de sécurité réseau

LAB:

- Lab 1: Configure AAA and Secure Remote Administration
- Lab 2: Configure Secure Network Management Protocols
- Lab 3: Configure Secure E1C3RP Routing
- Lab 4: Configure Secure Layer 2 Infrastructure
- Lab 5: Configure DHCP Snooping and STP Protection
- Lab 6: Configure Interfaces and NAT on the Cisco ASA
- Lab 7: Configure Network Access Control with the Cisco ASA
- Lab 8: Configure Site-to-Site VPN on IOS
- Lab 9: Configure Any Connect Remote Access VPN on ASA
- Lab 10: Configure Clientless SSL VPN on the ASA

CERTIFICATION:

Cette formation prépare à la certification *210-260 IINS*.

COURS SUIVANT:

Implementing Cisco Secure Mobility

Mettre en œuvre les solutions Cisco Secure Access

Implementing Cisco Threat Control Systems