Implementing Cisco IOS Network Security

IINS

In diesem Kurs lernen Sie schwerpunktmäßig den Entwurf, die Implementierung und die Überwachung einer umfassenden Sicherheitsrichtlinie mit Cisco IOS Sicherheitsfeatures und –technologien und deckt die Security Controls von Cisco IOS Devices sowie eine Einführung in die Funktionen der Cisco ASA Adaptive Security Appliance. Der Kurs ermöglicht Ihnen durch die Nutzung von trainergeleiteten Diskussionen, Vorträgen und praktischen Lab-Übungen grundlegende Aufgaben durchzuführen, um das Netzwerk einer kleinen Zweigstelle mit Cisco IOS Sicherheitsfeatures, die über Web-basierte GUIs verfügbar sind, und dem CLI auf Cisco Routern, Switches und ASA Appliances, abzusichern.

Nach Abschluss des Kurses werden die Teilnehmen folgende Aufgaben erfüllen können:

- Beschreibung der Komponenten einer umfassenden Netzwerk-Sicherheitsrichtlinie, die gegen Bedrohungen der IT-Systeme im Kontext des Security Policy Life Cycle genutzt werden können
- Entwicklung und Implementierung von Sicherheits-Gegenmaßnahmen, mit dem Ziel, Netzwerkelemente als Teil der Netzwerkinfrastruktur zu schützen.
- Einsatz und Wartung von Bedrohungskontrolle- und -Eindämmungstechnologien für die Sicherung von Netzwerken kleiner und mittlerer Größe
- Beschreibung sicherer Connectivity-Strategien und -Technologien mit VPNs sowie die Konfigurierung von Site-to-Site und Fernzugriffs-VPNs mit Cisco IOS Features

Zielgruppe

Netzwerkadministratoren und Techniker, die Cisco Network Security Produkte installieren und verwalten sollen.

Kerninhalte

- Examining Network Security Fundamentals
- Building Cisco Self-Defending Networks
- Configuring AAA on a Cisco Router using the Local Database
- Locking Down the Router
- Creating Static Packet Filters using ACLs
- Examining Cryptographic Services
- Building a Site-To-Site IPSec VPN
- Introducing IPS Technologies
- Configuring Cisco IOS IPS using Cisco SDM
- Mitigating Layer 2 Attacks

Voraussetzungen

Der Kurs ICND1 und ICND2 muss bereits besucht worden sein oder adequate IOS Kenntnisse müssen vorhanden sein.
Um den CCNA Security zu erlangen, muss die CCNA Prüfung erfolgreich absolviert worden sein.

Modul 1: Grundlagen der Netzwerksicherheit
- Lektion 1: Vorstellung von Netzwerksicherheitskonzepten
- Lektion 2: Verständnis von Sicherheitspraktiken unter Nutzung eines Life-Cycle-Ansatzes
- Lektion 3: Aufbau einer Sicherheitsstrategie für Borderless Networks

Modul 2: Schutz der Netzwerkinfrastruktur
- Lektion 1: Einführung in Cisco Network Foundation Protection
- Lektion 2: Schutz der Netzwerkinfrastruktur mit Cisco Configuration Professional
- Lektion 3: Sicherung der Management-Ebene auf Cisco IOS Devices
- Lektion 4: Konfiguration von AAA auf Cisco IOS Devices mit Cisco Secure ACS
- Lektion 5: Sicherung der Data Plane auf Cisco Catalyst Switches
- Lektion 6: Sicherung der Data Plane in IPv6 Umgebungen

Modul 3: Bedrohungskontrolle und -Eindämmung
- Lektion 1: Planung einer Strategie zur Bedrohungskontrolle
- Lektion 2: Implementierung von Access Control Listen zur Bedrohungs-Minderung
- Lektion 3: Verständnis der Firewall-Grundlagen
- Lektion 4: Implementierung von Cisco IOS Zone-Based Policy Firewalls
- Lektion 5: Konfiguration von Basis-Firewall-Richtlinien auf Cisco ASA Appliances
- Lektion 6: Verständnis der IPS-Grundlagen
- Lektion 7: Implementierung von Cisco IOS IPS

Modul 4: Sichere Connectivity
- Lektion 1: Verständnis der Grundlagen der VPN Technologien
- Lektion 2: Vorstellung der Public Key Infrastruktur
- Lektion 3: Examining IPsec Fundamentals
- Lektion 4: Implementierung von Site-to-Site VPNs auf Cisco IOS Routern
- Lektion 5: Implementierung von SSL VPNs mit Cisco ASA Appliances

Weiterführung
SNAF - Securing Networks with ASA Fundamentals (BACKUP)

Bemerkungen
Kursunterlagen und -setup: Englisch
Kurssprache: Deutsch

Um den CCNA Security zu erlangen, muss die CCNA Prüfung erfolgreich absolviert worden sein.

Dieser Kurs findet in Zusammenarbeit mit unserem Partner Fast Lane Institute for Knowledge Transfer GmbH statt.

Dauer
5 Tage