
Implementing Cisco Intrusion Prevention System

Dauer: 5 Tage **Kurscode: IPS**

Kursbeschreibung:

Im Cisco IPS Kurs werden die erforderlichen Kenntnisse und Fähigkeiten für den Einsatz einer IPS Lösung für die verschiedenen Unternehmensnetze vermittelt.

Der Kursinhalt beschäftigt sich mit der Implementierung des Sensors im Netzwerk (Design), sowie der Konfiguration und das Anpassen des Sensors im Netzwerk. Die Konfiguration des Sensor basiert auf dem IDM (IPS Device Manager), desweiteren wird der Cisco Event Viewer (IEV) behandelt und Events auszuwerten bzw. Reporting zu betreiben.

Desweiteren werden in diesem Kurs auch die neuen Features des 7.x Release behandelt, wie z.B. Virtual Sensor.

Alle Übungen basieren auf der IPS Serie 42xx, desweiteren wird auch in dem Kurs auf das ISDM-2 Modul (Catalyst 6500 Serie) und das AIP-SSM (ASA) eingegangen.

Zielgruppe:

Netzwerkadministratoren und Techniker, die Cisco Network Security Produkte installieren und verwalten sollen. Kandidaten für die CCNP Security Zertifizierung.

Kursziele:

- s. Schulungsinhalt
-

Voraussetzungen:

- Erfahrung mit der Konfiguration der Cisco IOS Software
- Gute Kenntnisse vom TCP/IP Stack in der LAN/WAN Umgebung
- Basiskenntnisse über Betriebssysteme (z.B. Windows)
- Kenntnisse im Netzwerk-/Security-Umfeld im speziellen Angriffe und Attacken aus dem Netzwerk

Tests und Zertifizierungen

Dieser Kurs bereitet Sie auf die Cisco Certified Network Professional for Security (CCNP Security) Zertifizierung vor. Erforderlich für die Händler-Akkreditierung zum Cisco Security Specialist Partner und zum Cisco Advanced Security Specialist Partner.

Folgekurse:

- Deploying Cisco ASA VPN Solutions (VPN)
-

Schulungsinhalt:

Introduction to Intrusion Prevention and Detection, Cisco IPS Software, and Supporting Devices

- Evaluating Intrusion Prevention and Intrusion Detection Systems
- Choosing Cisco IPS Software, Hardware, and Supporting Applications
- Evaluating Network IPS Traffic Analysis Methods, Evasion Possibilities, and Anti-Evasive Countermeasures
- Choosing a Network IPS and IDS Deployment Architecture

Installing and Maintaining Cisco IPS Sensors

- Integrating the Cisco IPS Sensor into a Network
- Performing the Cisco IPS Sensor Initial Setup
- Managing Cisco IPS Devices

Applying Cisco IPS Security Policies

- Configuring Basic Traffic Analysis
- Implementing Cisco IPS Signatures and Responses
- Configuring Cisco IPS Signature Engines and the Signature Database
- Deploying Anomaly-Based Operation

Adapting Traffic Analysis and Response to the Environment

- Customizing Traffic Analysis
- Managing False Positives and False Negatives
- Improving Alarm and Response Quality

Managing and Analyzing Events

- Installing and Integrating Cisco IPS Manager Express with Cisco IPS Sensors
- Managing and Investigating Events Using Cisco IPS Manager Express
- Using Cisco IME Reporting and Notifications
- Integrating Cisco IPS with Cisco Security Manager and Cisco Security MARS
- Using the Cisco IntelliShield Database and Services

Deploying Virtualization, High Availability, and High Performance Solutions

- Using Cisco IPS Virtual Sensors
- Deploying Cisco IPS for High Availability and High Performance

Configuring and Maintaining Specific Cisco IPS Hardware

- Configuring and Maintaining the Cisco ASA AIP SSM and AIP SSC Modules
- Configuring and Maintaining the Cisco ISR IPS AIM and IPS NME Modules
- Configuring and Maintaining the Cisco IDSM-2 Module

Labs

- Lab 2-1: Performing the Cisco IPS Sensor Initial Setup
- Lab 2-2: Managing a Cisco IPS Sensor
- Lab 3-1: Configuring and Modifying Basic Cisco IPS Signatures and Responses
- Lab 3-2: Configuring Cisco IPS Anomaly-Based Operation
- Lab 4-1: Configuring Custom Cisco IPS Signatures
- Lab 4-2: Managing False Positives and False Negatives
- Lab 4-3: Improving Alarm and Response Quality
- Lab 5-1: Using the Cisco IME
- Lab 5-2: Using Cisco IPS and Security Intelligence Web Resources
- Lab 6-1: Configuring Policy Virtualization

Hinweis:

Schulungsunterlagen: Original Cisco (englisch)
Methoden: Vortrag und praktische Übungen

Weitere Informationen:

Für weitere Informationen oder Buchung kontaktieren Sie uns bitte unter 0800 / 295 26 33

info@globalknowledge.de

www.globalknowledge.de

Global Knowledge Germany Training GmbH, Friedensallee 271, 22763 Hamburg