Implementing Cisco Intrusion Prevention System (IPS)

Course ID#: 1575-946-ZZ-W
Hours: 35

Course Content

Course Description:

The Implementing Cisco Intrusion Prevention System (IPS) course is part of the curriculum path leading to the Cisco Certified Network Professional Security (CCNP Security) certification. It is a five-day instructor-led course aimed at providing network security engineers with the knowledge and skills needed to deploy Cisco IPS-based security solutions. Successful graduates will be able to reduce risk to the IT infrastructure and applications using Cisco IPS features, and provide detailed operations support for the Cisco IPS.

Prerequisites:

Cisco Certified Network Associate (CCNA) certification

- Interconnecting Cisco Network Devices 1 (ICND1)
- Interconnecting Cisco Network Devices 2 (ICND2)
- Cisco Certified Network Associate Security (CCNA Security) certification
- Implementing Cisco IOS Network Security (IINS)
- Working knowledge of the Microsoft Windows operating system

Topics:

Module 1: Introduction to Intrusion Prevention and Detection, Cisco IPS Software, and Supporting Devices

Lesson 1: Evaluating Intrusion Prevention and Intrusion Detection Systems

- Intrusion Detection versus Intrusion Prevention
- Intrusion Prevention Terminology
- Network IPS o Endpoint Security Controls

Lesson 2: Choosing Cisco IPS Software, Hardware, and Supporting Applications

- Cisco IPS Network Sensors
- Cisco IPS Software Architecture
- Cisco IPS Management Products
- Cisco SIO and Cisco Security IntelliShield Alert Manager Service

Lesson 3: Evaluating Network IPS Traffic Analysis Methods, Evasion Possibilities, and Anti- Evasive Countermeasures

- Network IPS Traffic Analysis Methods
- Network IPS Evasion Techniques

Lesson 4: Choosing a Network IPS and IDS Deployment Architecture

- Sensor Deployment Considerations
- Implementing IPS at the Enterprise Internet Edge
- Implementing IPS in WANs
- Implementing IPS in Data Centers o Centralized Sensor Deployment

Implementing Cisco Intrusion Prevention System (IPS)

Course ID#: 1575-946-ZZ-W

Hours: 35

Module 2: Installing and Maintaining Cisco IPS Sensors

Lesson 1: Integrating the Cisco IPS Sensor into a Network

- Deploying Sensors in Promiscuous Mode
- Deploying Sensors in Inline Interface Pair Mode
- Deploying Sensors in Inline VLAN Pair Mode
- Deploying Sensors in Inline VLAN Group Mode
- Deploying Sensors in Selective Inline Analysis Mode

Lesson 2: Performing the Cisco IPS Sensor Initial Setup

- Using the Cisco IPS Sensor CLI
- Initializing the Cisco IPS Sensor
- Introducing the Cisco IPS Device Manager
- Configuring Cisco IPS Sensor Interfaces
- Troubleshooting the Initial Cisco IPS Sensor Configuration
- Troubleshooting Cisco IPS Hardware o Restoring Default Settings

Lesson 3: Managing Cisco IPS Devices

- Managing Basic Cisco IPS Sensor Device Features o Managing Users and Remote Management Channels
- Managing Cisco IPS Licensing
- Upgrading and Recovering Cisco IPS Sensor Software o Updating Cisco IPS Signatures
- Recovering System Passwords
- Monitoring Cisco IPS Sensor Health and Performance

Module 3: Applying Cisco IPS Security Policies

Lesson 1: Configuring Basic Traffic Analysis

- Configuring the Default Virtual Sensor
- Understanding Cisco IPS Sensor Inline Traffic Normalization
- Configuring Cisco IPS Sensor Promiscuous Mode Traffic Reassembly Options
- Configuring TCP Session Tracking
- Understanding IPv6 Support in Cisco IPS Sensors
- Choosing and Configuring Cisco IPS Sensor Bypass

Lesson 2: Implementing Cisco IPS Signatures and Responses

- Cisco IPS Signatures
- Configuring Basic Signature Properties
- Configuring Signature Actions
- Configuring Remote Blocking
- Configuring Packet Capture and IP Logging
- Understanding Threat and Risk Rating
- Understanding and Configuring Event Action Overrides
- Using Event Action Filters
- Choosing an Action Configuration Strategy
- Examining Alerts in IPS Event Logs

Implementing Cisco Intrusion Prevention System (IPS)

Course ID#: 1575-946-ZZ-W
Hours: 35

Lesson 3: Configuring Cisco IPS Signature Engines and the Signature Database
- Using Cisco IPS Signature Engines and Configuring Common Signature Engine
- Parameters
- Deploying ATOMIC Signature Engines
- Deploying STRING Signature Engines
- Deploying SERVICE Signature Engines
- Deploying FLOOD Signature Engines
- Deploying SWEEP Signature Engines
- Deploying the META Signature Engine
- Deploying the NORMALIZER Engine
- Deploying Other Engines

Lesson 4: Deploying Anomaly-Based Operation
- Anomaly Detection Overview
- Anomaly Detection Components
- Configuring Anomaly Detection
- Monitoring and Troubleshooting Anomaly Detection

Module 4: Adapting Traffic Analysis and Response to the Environment

Lesson 1: Customizing Traffic Analysis
- Creating Custom Signatures
- Using the Custom Signature Wizard
- Using the Custom Signature Wizard Without Specifying a Signature Engine
- Manually Configuring Custom Signatures

Lesson 2: Managing False Positives and False Negatives
- Tuning False Positives and False Negatives
- Tuning the Cisco IPS Sensor to Reduce False Positives
- Tuning the Cisco IPS Sensor to Reduce False Negatives

Lesson 3: Improving Alarm and Response Quality
- Deploying Sensor Features to Improve the Quality of Prevention and Detection
- Deploying Operating System Identification
- Using Target Value Ratings
- Using Signature Fidelity Ratings
- Using Management Center for Cisco Security Agent Attacker Information
- Deploying Global Correlation and Reputation-Based Filtering

Module 5: Managing and Analyzing Events

Lesson 1: Installing and Integrating Cisco IPS Manager Express with Cisco IPS Sensors
- Cisco IPS Manager Express Overview
- Installing Cisco IPS Manager Express
- Using and Customizing the Cisco IPS Manager Express User Interface
- Integrating Cisco IPS Manager Express with Cisco IPS Sensors

Lesson 2: Managing and Investigating Events Using Cisco IPS Manager Express
- Managing IPS Events Using Cisco IPS Manager Express
- Investigating IPS Events Using Cisco IPS Manager Express
- Acting on IPS Events Using Cisco IPS Manager Express
- Exporting, Importing, and Archiving Events

Lesson 3: Using Cisco IME Reporting and Notifications
- Using Event Reporting in Cisco IME
- Using Notifications in Cisco IME

Implementing Cisco Intrusion Prevention System (IPS)

Course ID#: 1575-946-ZZ-W
Hours: 35

Lesson 4: Integrating Cisco IPS with Cisco Security Manager and Cisco Security MARS
- Configuring Integration with Cisco Security Manager
- Configuring Integration with Cisco Security MARS

Lesson 5: Using the Cisco IntelliShield Database and Services
- Using Cisco Security Intelligence Operations
- Using the Cisco IntelliShield Alert Manager Service

Module 6: Deploying Virtualization, High Availability, and High Performance Solutions

Lesson 1: Using Cisco IPS Virtual Sensors
Sensor Policy Virtualization Overview
- Adding and Configuring Virtual Sensors
- Verifying Virtual Sensor Operation

Lesson 2: Deploying Cisco IPS for High Availability and High Performance
- High-Availability Solutions for Cisco IPS Deployments
- Switching-Based Sensor High Availability
- Routing-Based Sensor High Availability
- Cisco ASA Security Appliance-Based Sensor High Availability
- Cisco IPS Sensor Performance Overview
- Increasing Performance Using Load Sharing
- Increasing Performance Using Traffic Reduction

Module 7: Configuring and Maintaining Specific Cisco IPS Hardware

Lesson 1: Configuring and Maintaining the Cisco ASA AIP-SSM and AIP-SSC-5
Modules
- Overview of Cisco ASA AIP-SSM and AIP-SSC Modules
- Initializing the Cisco ASA AIP-SSM and AIP-SSC Modules
- Integrating Cisco AIP-SSM and AIP-SSC Traffic Analysis with the Cisco ASA
- Adaptive Security Appliance
- Troubleshooting Cisco ASA AIP-SSM and AIP-SSC Modules

Lesson 2: Configuring and Maintaining the Cisco ISR IPS AIM and IPS NME Modules
- Cisco ISR IPS AIM and IPS NME Overview
- Initializing the Cisco ISR IPS AIM and IPS NME
- Integrating Cisco ISR IPS AIM and IPS NME Traffic Analysis with the Cisco ISR
- Troubleshooting Cisco ISR IPS AIM and IPS NME

Lesson 3: Configuring and Maintaining the Cisco IDSM-2
- Cisco IDSM-2 Overview
- Initializing the Cisco IDSM-2
- Integrating Cisco IDSM-2 Traffic Analysis with the Catalyst 6500 Series Switch
- Maintaining the Cisco IDSM-2
- Troubleshooting the Cisco IDSM-2