Implementing Cisco Intrusion Prevention System

Length
4 days

Format
Lecture/lab

Version
6.0

Course Description

This course teaches the knowledge and skills needed to design, install, and configure a Cisco Intrusion Prevention Solution (IPS) for small, medium, and enterprise networks.

The course covers Cisco IPS platforms including the Cisco 4200 series sensors, the Catalyst 6500 series Intrusion Detection System Module 2 (IDSM2), and the Network Module for Cisco 2600/3600/3700 Routers and Cisco 2800/3800 Integrated Services Routers. The IPS Device Manager is used to configure and manage Cisco IPS sensor platforms and view and respond to IPS alarms.

Who Should Attend

This course is designed for anyone tasked with implementing or maintaining a secure network using Cisco IPS solutions.

Recommended Prerequisites

- CCNA certification or equivalent knowledge
- Basic knowledge of the Windows operating system
- Securing Cisco Network Devices (SND)

Related Courses

- Introduction to Cisco Networking Technologies (INTRO)
- Interconnecting Cisco Network Devices (ICND)
- Securing Cisco Network Devices (SND)

IPS

Learning Objectives

After completing this course, you will be able to:

- Explain how Cisco IPS protects network devices from attacks
- Install a sensor appliance in the network
- Perform basic sensor configuration
- Describe the capabilities of the IPS Device Manager
- Use the IDM to configure the sensor's communication parameters, to configure allowed hosts, to set the sensor's time, to create user accounts, and to configure sensor interfaces and interface pairs
- Describe signature engines
- Use the IDM to tune and create signatures to meet security policy requirements
- Use the IDM to tune the sensor
- Explain blocking concepts
- Use the IDM to configure blocking
- Install the NM-CIDS in a router
- Configure communications between the router and the NM-CIDS
- Install an IDSM-2 in a Cisco Catalyst 6500 switch and initialize it
- Use the IDM to upgrade the sensor image, to install updates, and to configure automatic software updates
- Back up and restore sensor configuration
- Use CLI and IDM to monitor the sensor
- Use troubleshooting commands

Implementing Cisco Intrusion Prevention System

Course Outline

Module 1: Intrusion Prevention Overview

Lesson 1: Explaining Intrusion Prevention
Intrusion Detection vs. Intrusion Prevention
Intrusion Prevention Technologies
Intrusion Prevention Terminology
Promiscuous and Inline Modes
Features of Cisco IPS Sensor Software Version 6.0

Lesson 2: Examining Cisco IPS Products
Cisco Network Sensors
Network IPS
Host-Based IPS
Sensor Deployment
Cisco Self-Defending Network

Lesson 3: Examining Cisco IPS Sensor Software Solutions
Cisco IPS Sensor Software Architecture
Cisco IPS Element Management Products
Cisco IPS Enterprise Management Products

Lesson 4: Examining Evasive Techniques
Evasive Techniques
String Match Attacks
Fragmentation Attacks
Session Attacks
Insertion Attacks
Evasion Attacks
TTL-Based Attacks
Encryption-Based Attacks
Resource Exhaustion Attacks

Module 2: Installation of a Cisco IPS 4200 Series Sensor

Lesson 1: Installing a Cisco IPS Sensor Using the CLI
Introducing the CLI
Initializing the Sensor
Performing Administrative Tasks
Additional Administrative Commands

Lesson 2: Using the Cisco IDM
Introducing the Cisco IDM
Getting Started with the Cisco IDM
How to Configure SSH
How to Reboot and Shut Down the Sensor

Lesson 3: Configuring Basic Sensor Settings
How to Configure Allowed Hosts
How to Set the Time
How to Configure Certificates
How to Configure User Accounts
Defining Interface Roles
How to Configure the Interfaces
How to Configure Software and Hardware Bypass Mode
Viewing Events in the Cisco IDM

Module 3: Cisco IPS Signatures

Lesson 1: Configuring Cisco IPS Signatures and Alerts
Cisco IPS Signatures
How to Locate Signature Information
How to Configure Basic Signatures
Special Considerations for Signature Actions

Lesson 2: Examining the Signature Engines
Introducing Cisco IPS Signature Engines
Common Signature Engine Parameters
ATOMIC Signature Engines
FLOOD Signature Engines
SERVICE Signature Engines
STRING Signature Engines
SWEEP Signature Engines
TROJAN Signature Engines
TRAFFIC Signature Engines
AIC Signature Engines
STATE Signature Engine
META Signature Engine
NORMALIZER Engine

Lesson 3: Customizing Signatures
Tuning Signatures
Noise Reduction
False Positive Reduction
False Negative Reduction
Focusing Cisco IPS Sensors
Customizing Built-in Signatures
How to Create Custom Signatures
Custom Signature Scenarios

Implementing Cisco Intrusion Prevention System

Course Outline

Module 4: Advanced Cisco IPS Configuration

Lesson 1: Performing Advanced Tuning of Cisco IPS Sensors
Sensor Configuration
IP Logging
Reassembly Options
How to Define Event Variables
Target Value Rating
Event Action Overrides
Event Action Filters
Risk Rating System
General Settings of Event Action Rules

Lesson 2: Monitoring and Managing Alarms
Cisco IEV Overview
Installing Cisco IEV
Configuring Cisco IEV
Viewing Events
Cisco Security Management Suite Overview
External Product Interface
Integrating Cisco Security Agent into an IPS Installation
Cisco ICS

Lesson 3: Configuring a Virtual Sensor
Virtual Sensor Overview
Preparing for Virtual Sensors
Creating Virtual Sensors

Lesson 4: Configuring Advanced Features
Anomaly Detection Overview
Anomaly Detection Components
Configuring Anomaly Detection
Monitoring Anomaly Detection
POSFP Overview
Operating System Identification
Configuring POSFP
Monitoring POSFP

Lesson 5: Configuring Blocking
Blocking Overview
ACL Considerations
How to Configure Automatic Blocking
How to Configure Manual Blocking
How to Configure a Master Blocking Scenario

Module 5: Additional Cisco IPS Devices

Lesson 1: Installing the Cisco Catalyst 6500 Series IDSM-2
Cisco Catalyst 6500 Series IDSM-2 Overview
Installing the Cisco Catalyst 6500 Series IDSM-2
Configuring Cisco Catalyst 6500 Series IDSM-2 Interfaces
Monitoring the Cisco Catalyst 6500 Series IDSM□2
Maintaining the Cisco Catalyst 6500 Series IDSM-2

Lesson 2: Initializing the Cisco ASA AIP-SSM
Cisco ASA AIP-SSM Overview
Loading the Cisco ASA AIP-SSM
Initial Cisco ASA AIP-SSM Configuration Using Cisco ASDM
Configuring an IPS Security Policy

Lesson 5: Configuring System Correlation Rules
System Correlation Rules
How to Configure the System API Control Rule
Configuring the System API Control Rule
How to Configure the Network Shield Rule
How to Configure the Buffer Overflow Rule
The E-mail Worm Protection Module
The Installation Applications Policy
How to Configure Global Event Correlation

Module 6: Cisco IPS Sensor Maintenance

Lesson 1: Maintaining Cisco IPS Sensors
Understanding Cisco IPS Licensing
How to Upgrade and Recover Sensor Images
How to Install Service Packs and Signature Updates
Password Recovery
How to Restore a Cisco IPS Sensor

Lesson 2: Managing Cisco IPS Sensors
Using the CLI to Monitor the Sensor
Using the Cisco IDM to Monitor the Sensor
Monitoring Using Cisco Security Manager
Monitoring Using SNMP

CISCO PARTNER Learning Solutions

Implementing Cisco Intrusion Prevention System

Course Labs

Lab 2-1: Install and Configure a Cisco IPS Sensor from the CLI

Lab 2-2: Use the Cisco IDM to Perform a Basic Sensor Configuration

Lab 3-1: Working with Signatures and Alerts

Lab 3-2: Customizing Signatures

Lab 4-1: Tune a Cisco IPS Sensor Using the Cisco IDM

Lab 4-2: Monitor and Manage Alarms

Lab 4-3: Configure a Virtual Sensor (Optional)

Lab 4-4: Configure Anomaly Detection and POSFP

Lab 6-1: Maintain Sensors and Verify System Configuration