

Cisco Networks Implementing Cisco Intrusion Prevention System (IPS)

Course:ET934

Course Description

In this course, you will gain the skills required to deploy Cisco's recently updated version 5.0 network-based intrusion prevention system. New features added to version 5.0 include in-line protection, meta-event generation, and the application firewall. The course introduces you to Cisco IDS detection platforms including the 4200 Series Sensors, the Catalyst 6000 Series Intrusion Detection Module 2 (IDSM2), and the IDS Network Module (NM-CIDS). The command line and the IPS Device Manager GUI are used to configure the sensor

Who should attend?

Internetwork professionals who want to ensure security on their network or who seek Cisco certification. This course is also recommended for anyone pursuing the certification opportunities, including Cisco Certified Security Professional (CCSP™).

Pre-requisites

- Cisco Certified Network Associate (CCNA) certification
- Working knowledge of the Windows operating system
- Working knowledge of Cisco IOS networking and concepts

Course Objectives

- Describe the basic intrusion prevention terminology
- Explain the different intrusion prevention technologies and evasive techniques
- Design a Cisco IPS solution for small, medium, and enterprise customers
- Identify the Cisco IPS sensor platforms and describe their features
- Install and configure a Cisco IPS sensor
- Tune Cisco IPS signatures to work optimally in unique network environments
- Create and implement customized intrusion prevention signatures
- Create alarm exceptions to reduce alarms and possible false positives
- Configure a Cisco IPS sensor to perform device management of supported blocking devices
- Describe the Cisco IPS signatures and determine the immediate threat posed to the network
- Perform maintenance operations such as signature updates and software upgrades
- Describe the Cisco IPS architecture, including supporting services and configuration files

Course Outline

1. Defining Security Fundamentals
 - Need for Network Security
 - Network Security Policy
 - Primary Network Threats and Attacks
 - Reconnaissance Attacks and Mitigation
 - Access Attacks and Mitigation
 - Denial of Service Attacks and Mitigation
 - Worm, Virus, and Trojan Horse Attacks and Mitigation
 - Management Protocols and Functions
2. Explaining Intrusion Prevention
 - Intrusion Detection Vs Intrusion Prevention
 - Intrusion Detection Technologies
 - Intrusion Detection Evasive Techniques
 - Cisco Network Sensors
 - Sensor Appliances
 - Promiscuous and Inline Modes
 - Cisco Defense in Depth
 - Sensor Deployment
 - Intrusion Prevention Terminology
 - Cisco IPS Software Architecture
3. Getting Started with the IPS Command-Line Interface
 - CommandLine Overview
 - Sensor Installation
 - Sensor Initialization
 - Administrative Tasks
 - Basic Troubleshooting Commands
4. Using IPS Device Manager
 - Introduction to IPS Device Manager
 - Getting Started with the IDM
 - Configuring Certificates
 - Configuring SSH
 - Rebooting and Shutting Down the Sensor
 - Viewing Events in the IDM
5. Configuring the Sensor
 - Configuring Allowed Hosts
 - Setting the Time
 - Configuring User Accounts
 - Configuring the Interfaces
 - Configuring Software Bypass Mode
6. Working with Signatures and Alerts
 - Cisco IPS Signatures
 - Locating Signature Information
 - Basic Signature Configuration
 - Special Considerations for Signature Actions
 - Understanding and Configuring SNMP Support
7. Describing Signature Engines
 - Cisco IPS Signature Engines
 - Atomic Signature Engine
 - Flood Signature Engines
 - Meta Signature Engine
 - Normalizer Engine
 - Service Signature Engines
 - State Signature Engine

- String Signature Engines
 - Sweep Signature Engines
 - Traffic and Trojan Signature Engines
 - AIC Signature Engines
8. Configuring Signatures
 - Parameters Common to All Signature Engines
 - Signature Tuning
 - Creating Custom Signatures
 9. Tuning the Sensor
 - Tuning the Sensor
 - Logging
 - Reassembly Options
 - Event Action Rules
 - Event Variables
 - Target Value Rating
 - Event Action Overrides
 - Event Action Filters
 - General Settings
 - Configuring Blocking
 - ACL Considerations
 - Automatic Blocks
 - Manual Blocks
 - Master Blocking Sensors
 10. Maintaining the Sensor
 - Upgrading and Recovering the Sensor Image
 - Service Pack and Signature Updates
 - Resetting, Powering Down, and Restoring the Default Configuration
 11. Monitoring the Sensor
 - Using the CLI to Monitor the Sensor
 - Using the IDM to Monitor the Sensor
 12. Installing and Maintaining the NM-CIDS
 - How the NM-CIDS Works
 - Design Considerations
 - Installation and Configuration Tasks
 - Image Upgrade and Recovery
 - Maintenance Tasks Unique to the NM-CIDS
 13. Installing and Maintaining the IDSM-2
 - Ports, Traffic, and Time
 - Installation and Configuration Tasks
 - Verifying IDSM-2 Status
 - Upgrade and Recovery

Labs

- Lab 1: Initialize the Sensor
- Lab 2: The IPS Command Line
- Lab 3: Introduction to IDM
- Lab 4: Configuring the Sensor
- Lab 5: Working with Signatures
- Lab 6: Study Built-In Signatures Lab
- Lab 7: Signature Configuration
- Lab 8: Sensor Tuning
- Lab 9: Blocking
- Lab 10: Sensor Maintenance

Register Now 02-260-3233
<http://www.ctt-center.com>

Certifeid Technical Training Center Co.,Ltd