Securing Hosts Using Cisco Security Agent

Length
2 days

Format
Lecture/lab

Version
3.0

Course Description

The Cisco Security Agent protects networks from intrusions, as compared to simply detecting attempted intrusions. HIPS is a lab-intensive course that takes a task-oriented approach to teach the knowledge and skills to deploy, configure, and administer the Cisco Security Agent.

Who Should Attend

This course is designed for network professionals who need to implement or maintain intrusion protection services.

Recommended Prerequisites

- CCNA certification or equivalent knowledge
- CSSI certification, *or* the Cisco Firewall, IDS, and VPN Specialist certifications
- At least 6 months practical experience configuring Cisco IDS Sensors
- Competency in using Windows server operating systems
- Familiarity with network security policies and concepts

Related Courses

- Introduction to Cisco Networking Technologies (INTRO)
- Interconnecting Cisco Network Devices (ICND)
- Securing Networks with PIX and ASA (SNPA)
- Implementing Cisco Intrusion Prevention System (IPS)
- Cisco Secure Virtual Private Networks (CSVPN)

HIPS

Learning Objectives

After completing this course, you will be able to:

- Understand attack types and methods, and the Cisco security wheel
- Describe CSA functionality, components, and architecture
- Describe CSAMC installation and system requirements for management console
- Understand CSAMC configuration
- Access and use management console
- Configure groups, manage hosts, build agent kits, distribute software updates
- Develop a security policy; configure policies and rules for Windows and UNIX
- Use system correlation and heuristics
- Understand/configure application classes
- Configure variables: file sets, network address sets, network services, registry sets, and COM component sets
- Use CSA Profiler
- Configure and manage event logging, alerts, and reports
- Understand and use CSAMC utilities: start/stop service for servers and agent, webmgr utility, backup configurations, COM extract utility, and export/import

CISCO PARTNER
Learning Solutions

Securing Hosts Using Cisco Security Agent

Course Outline

Module 1: Configuring CSA

Lesson 1: Introducing CSA
What Is the Cisco SDN Strategy?
CSA in the Multilayered Cisco SDN Strategy
The CSA Architecture
Handling System Calls
Handling a Network Attack
Features of CSA
CSA MC Building Blocks

Lesson 2: Installing and Configuring CSA MC
Requirements for Installing CSA MC
How to Install CSA MC
How to Access the CSA MC Interface
The CSA MC Interface
How to Configure CSA MC
Requirements for Installing CSA
How to Install CSA

Module 2: Configuring Groups and Policies

Lesson 1: Configuring Groups
Groups
How to Configure a Group
How to Generate and Distribute Rule Programs

Lesson 2: Building an Agent Kit
Agent Kits
How to Build an Agent Kit
About Installing and Uninstalling Agents
Using Scripts
How to Control the Registration of Hosts

Lesson 3: Managing Hosts and Deploying Software Updates
Host Information Management
How to Add a Host to a Group
How to Deploy Scheduled Software Updates
Practice: Deploying Software Updates

Lesson 4: Configuring Policies
What Is a Security Policy?
How to Configure a Policy
How to Configure a Rule Module
How to Set System and User State Conditions
How to Add a Rule to a Rule Module
How to View Rule Details
How to Compare Rule Modules
How to Attach a Rule Module to a Policy
How to Attach a Policy to a Group

Module 3: Working with Variables and Application Classes

Lesson 1: Creating Variables
Variables
How to Configure a Data Set
How to Configure a File Set
Practice: Configuring a File Set
How to Configure a Network Address Set
How to Configure a Network Services Set
How to Configure a Registry Set
How to Configure a COM Component Set
How to Configure Query Settings

Lesson 2: Creating Application Classes
Application Classes
What are Static and Dynamic Application Classes?
How to Configure an Application Class
Practice: Creating a Dynamic Application Class
How to Configure Application Class Management Options

Securing Hosts Using Cisco Security Agent

Course Outline

Module 4: Configuring Rules

Lesson 1: Rule Basics
Types of Rules
Rule Action List

Lesson 2: Configuring Rules Common to Windows and UNIX
Rules Common to Windows and UNIX Hosts
How to Configure the Agent Service Control Rule
How to Configure the Agent UI Control Rule
How to Configure the Application Control Rule
How to Configure the Connection Rate Limit Rule
How to Configure the Data Access Control Rule
How to Configure the File Access Control Rule
Practice: Configuring the File Access Control Rule Using the Set Action
How to Configure the Network Access Control Rule
Practice: Configuring an Application-Builder Rule

Lesson 3: Configuring Windows-Only Rules
Windows-Only Rules
How to Configure the Clipboard Access Control Rule
How to Configure the COM Component Access Control Rule
Practice: Configuring the COM Component Access Control Rule
How to Configure the File Version Control Rule
Practice: Configuring the File Version Control Rule
How to Configure the Kernel Protection Rule
How to Configure the NT Event Log Rule
How to Configure the Registry Access Control Rule
How to Configure the Service Restart Rule
How to Configure the Sniffer and Protocol Detection Rule

Lesson 4: Configuring UNIX-Only Rules
UNIX-Only Rules
How to Configure the Network Interface Control Rule
How to Configure the Resource Access Control Rule
How to Configure the Rootkit/Kernel Protection Rule
How to Configure the Syslog Control Rule

Lesson 5: Configuring System Correlation Rules
System Correlation Rules
How to Configure the System API Control Rule
Practice: 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 5: Administering Events and Generating Reports

Lesson 1: Managing Events
What Is Logging?
How to View Events Using the Event Log
How to View Events Using the Event Monitor
Event Log Management
The Event Management Wizard
How to Configure an Event Set
How to Configure an Alert
How to View System Summary Information

Lesson 2: Generating Reports
Types of Reports
How to Generate an Events by Severity Report
How to Generate an Events by Group Report
How to Generate a Group Detail Report
How to Generate a Host Detail Report
How to Generate a Policy Detail Report
How to View the Audit Trail

CISCO PARTNER Learning Solutions

Securing Hosts Using Cisco Security Agent

Course Outline

Module 6: Using CSA Analysis

Lesson 1: Configuring Application Deployment Investigation
Application Deployment Investigation
How to Configure Group Settings
How to Configure Product Associations
How to Configure Unknown Applications
How to Configure Data Management

Lesson 2: Generating Application Deployment Reports
Application Deployment Reports
How to Generate an Antivirus Installations Report
How to Generate an Installed Products Report
How to Generate an Unprotected Hosts Report
How to Generate an Unprotected Products Report
How to Generate a Product Usage Report
How to Generate a Network Data Flows Report
How to Generate a Network Server Applications Report

Lesson 3: Configuring Application Behavior Investigation
Application Behavior Investigation
How to Configure Behavior Analysis

Lesson 4: Generating Behavior Analysis Reports
Behavior Analysis Reports
How to View Behavior Analysis Reports
File Event Reports
Registry Event Reports
COM Event Reports
Network Event Reports
Summary Reports

Lab 1-1: Deploying CSA for the MCMB Network

Lab 2-1: Configuring Groups and Managing Hosts for the MCMB Network

Lab 2-2: Configuring a Policy for the MCMB Network

Lab 3-1: Creating Variables for the MCMB Network

Lab 3-2: Creating Application Classes for the MCMB Network

Lab 4-1: Configuring Rules for Windows Hosts in the MCMB Network

Lab 5-1: Using Event Logs and Generating Reports for the MCMB Network