
IMPLEMENTING INTRUSION DETECTION AND PREVENTION

Course No: EDU-JUN-IIDP

Length: 3 days

Course Overview

This three-day course discusses the configuration of Juniper Intrusion Detection and Prevention (IDP) sensors in a typical network environment. Key topics include sensor configuration, creating and fine-tuning security policies, managing attack objects, creating custom signatures, and troubleshooting. This course is based upon IDP software version 4.1 and Security Manager 2007.3.

Through demonstrations and hands-on labs, students will gain experience in configuring, testing, and troubleshooting the IDP sensor.

Objectives

After successfully completing this course, you should be able to:

- Deploy an IDP sensor on the network.
- Monitor and understand IDP logs.
- Configure, install, and fine-tune IDP policies.
- Configure the Profiler.
- Troubleshoot sensor problems.
- Create custom signature attack objects.
- Configure sensors for high availability using third-party devices.

Intended Audience

This course is intended for network engineers, support personnel, reseller support, and others responsible for implementing Juniper Networks IDP products.

Course Level

This is an introductory-level course.

Prerequisites

This course assumes that students have basic networking knowledge and experience in the following areas:

- Understanding of TCP/IP operation;
- Understanding of network security concepts;
- Experience in network security administration; and
- Experience in UNIX system administration.

It also assumes that students have attended the Juniper Networks *Security Manager Fundamentals* course.

Course Contents

Day 1

Chapter 1: Course Introduction

Chapter 2: Intrusion Detection and Prevention Concepts

- Network Attack Phases and Detection
- Juniper Networks IDP Product Offerings
- Juniper Networks IDP Three-Tier Architecture
- Juniper IDP Deployment Modes

Chapter 3: Initial Configuration of IDP Sensor

- Overview of IDP Sensor Deployment Process
- Initial Configuration Steps—IDP Standalone Device
- Initial Configuration Steps—ISG1000/ISG2000
- Lab 1: Sensor Initial Configuration

Chapter 4: IDP Policy Basics

- Attack Object Terminology
- IDP Rule Components
- IDP Rule-Matching Algorithm
- Terminal rules
- Lab 2: Configuring IDP Policies

Chapter 5: Fine-Tuning Policies

- Tuning Process Overview
- Step 1: Identifying Machines and Protocols to Monitor
- Step 2: Identifying and Eliminating False Positives
- Step 3: Identifying and Configuring Responses to Real Attacks
- Step 4: Configuring Other Rulebases to Detect Attacks
- Lab 3: Fine-Tuning IDP Policies

Day 2

Chapter 6: Configuring Additional Rulebases

- Overview of IDP-Related Rulebases
- Exempt Rulebases
- Traffic Anomalies Rulebase
- Backdoor Rulebase
- SYN Protector Rulebase
- Network Honeypot Rulebase
- Rulebase Processing Order
- Lab 4: Configuring Additional Rulebases

Chapter 7: Profiler

- Profiler Overview
- How to Operate Profiler
- Using Profiler for Network Discovery
- Using Profiler to Discover Running Applications
- Using Profiler to Detect New Devices and Ports
- Using Profiler to Detect Policy Violations
- Lab 5: Using Profiler

Chapter 8: Sensor Operation and Sensor Commands

- Main Components of the Sensor
- Description of Sensor Processes
- Managing Policies with the scio Utility
- Managing Sensor Configuration with the scio Utility
- Monitoring with the sctop Utility
- Lab 6: Using Sensor Commands

Chapter 9: Troubleshooting

- Review of Sensor Communication
- Troubleshooting Tools
- Troubleshooting Scenarios
- Reimaging the Sensor
- Lab 7: Troubleshooting

Day 3

Chapter 10: Managing Attack Objects

- Examining Predefined Attack Objects
- Examining Predefined Attack Object Groups
- Creating New Custom Attack Object Groups
- Updating the Attack Object Database
- Searching the Attack Object Database
- Lab 8: Managing Attack Objects

Chapter 11: Creating Custom Signatures

- IDP Packet Inspection
- Obtaining Attack Information
- Understanding Regular Expressions
- Creating a Signature-Based Attack Object
- Creating a Compound Attack Object
- Lab 9: Creating Custom Signatures

Chapter 12: Configuring Sensors for External High Availability

- External HA Operation
- Configuring Sensors for External HA

