Implementing Intrusion Detection and Prevention

Course 1740 – 24 Hours

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 4.0 and Security Manager 2006.1.

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

On Completion, Delegates will 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.

Who Should Attend

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

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 Security Manager Fundamentals (2-day) course

Course Contents

Course Introduction

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

Initial Configuration of IDP Sensor

- Overview of IDP Sensor Deployment Process
- Initial Configuration Steps
- Answers to Review Questions
- Lab 1: Sensor Initial Configuration

IDP Policy Basics

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

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

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

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

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

Troubleshooting

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

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

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

Configuring Sensors for External High Availability

- External HA Operation
- Configuring Sensors for External HA