ProTech *"Charting the Course ...*

protechtraining.com

... to Your Success!"

Securing Cisco Networks with Sourcefire Intrusion Prevention System (SSFIPS)

Course Summary

Description

Securing Cisco Networks with Sourcefire Intrusion Prevention System (IPS) is an instructor-led, lab-intensive course that introduces students to the powerful features of the Cisco Sourcefire System, including FireSIGHT technology, in-depth event analysis, IPS tuning and configuration, and the Snort rules language.

Students will learn how to use and configure next-generation Sourcefire technology, including application control, firewall, and routing and switching capabilities. Students will also learn to properly tune your system for better performance and greater network intelligence while taking full advantage of powerful tools for more efficient event analysis, including file type and network-based malware detection.

This course combines lecture materials and hands-on labs throughout to make sure that students are able to successfully deploy and manage the Sourcefire System.

Objectives

By the end of this course, students will be able to:

- Undertstand the Sourcefire System infrastructure
- Navigate the UI and administrative features of the Sourcefire System, including reporting functionality to properly assess threats
- Understand how to deploy and manage the Sourcefire device
- Understand the role FireSIGHT technology plays in the Sourcefire System
- Understand, create, and implement objects for use in access control policies
- Understand advanced policy configuration and Sourcefire System configuration options
- Analyze events
- Write and configure several basic rules

Topics

- Sourcefire System Overview and Classroom Setup
- Device Management
- Object Management
- Access Control Policy
- Network-based Malware Detection
- FireSIGHT Technology
- Correlation Policies
- IPS Policy Basics
- Advanced IPS Policy Configurations
- User Account Management
- Event Analyis
- Reporting
- Basic Rule Syntax and Usage
- Case Studies in Rule Writing and Packet Analysis

Audience

This course is designed for technical professionals who need to know how to deploy and/or manage a Sourcefire System in their work environment. The primary audience for this course includes:

- Security administrators
- Security consultants
- Network administrators
- System engineers
- Technical support personnel
- Channel partners and resellers

Securing Cisco Networks with Sourcefire Intrusion Prevention System (SSFIPS)

Course Summary (cont'd)

Prerequisites

It is recommended that prior to enrollment, students have the following:

- Technical understanding of TCP/IP networking and network architecture
- Basic familiarity with the concepts of intrusion detection systems (IDS) and IPS

Duration

Five days

ProTech "Charting the Course ...

protechtraining.com

... to Your Success!"

Securing Cisco Networks with Sourcefire Intrusion Prevention System (SSFIPS)

Course Outline

I. Sourcefire System Overview and Classroom Setup

II. Device Management

III. Object Management

IV. Access Control Policy

V. Network-based Malware Detection

VI. FireSIGHT Technology

VII. Correlation Policies

VIII. IPS Policy Basics

IX. Advanced IPS Policy Configurations

X. User Account Management

XI. Event Analyis

XII. Reporting

XIII. Basic Rule Syntax and Usage

XIV. Case Studies in Rule Writing and Packet Analysis

XV. Labs

A. Verifying the License
B. Testing the Environment by Running Attack PCAPs
C. Viewing Events
D. Layer 2 and 3 Simulation
E. Inline Interface Configuration
F. Creating Objects
G. Creating an Access Control Policy (Port Inspection)
H. Creating an Access Control Policy (Application Awareness)
I. URL Filtering
J. Including an IPS Policy in Access Control Rules
K. Creating a File Policy
L. Tuning the Network Discovery Policy
M. Viewing FireSIGHT Data
N. User Discovery
O. Creating a Correlation Policy Based on Connection Data
P. White Lists
Q. Working with Connection Data and Traffic Profiles
R. Creating an Intrusion Policy
S. Including FireSight Recommendations in an Intrusion Policy
T. Tuning Your HTTP_Inspect Preprocessor
U. Apply and Test Your Policy and Variable Set
V. Create User Accounts and Configure the UI Timeout Value
W. Testing Exempt and Non Exempt Users
X. Permission Escalation
Y. Working with External Accounts
Z. Analysis Lab
AA. Tuning Events
BB. Context Explorer
CC. Comparing Trends with Reports
DD. Writing Custom Rules
EE. Research and Packet Analysis
FF. Revisiting the Kaminsky Vulnerability