SSFIPS - Securing Cisco Networks with Sourcefire FireSIGHT Intrusion Prevention System v3.0

Code: 5593
Length: 4 days
URL: View Online

In this course, you will learn about basic next-generation intrusion prevention system (NGIPS) and firewall security concepts. You will learn about the Cisco Firepower system, its powerful features:

- In-depth event analysis
- NGIPS tuning and configuration
- Snort rules language

Yoll also become familiar with the latest platform features: file and malware inspection, security intelligence, domain awareness, and more.

The course begins by introducing the system architecture, the latest major features, and the role of policies in implementing the solution. You learn how to manage deployed devices and perform basic Cisco Firepower discovery. Yoll be able to describe how to use and configure Cisco NGIPS technology, including application control, security intelligence, firewall, and network-based malware and file controls. Yoll learn how to take advantage of powerful tools so you can carry out more efficient event analysis, including the detection of file type and network-based malware. And yoll learn how to properly tune systems for better performance and greater network intelligence. The course finishes with system and user administration tasks.

This course combines lecture materials and hands-on labs that will give you practice in deploying and managing the Cisco Firepower system.

Skills Gained

- Key features and concepts of NGIPS and firewall security
- Cisco Firepower system components, features, and high-level implementation steps
- Cisco Firepower Management Center GUI and understand the role of policies when configuring the Cisco Firepower system
- Deploy and manage Cisco Firepower managed devices
- Perform an initial Cisco Firepower discovery and basic event analysis to identify hosts, applications, and services
- Create the objects required as prerequisites to implementing access control policies
- Features and functionality of access control policies and the implementation procedures
- Concepts and implementation procedures of security intelligence
- Concepts and implementation procedures of file control and advanced malware protection
- Use Cisco Firepower recommendations to implement IPS policies

- Use of network analysis policies and the role of preprocessor technology in processing network traffic for NGIPS inspection
- Demonstrate the detailed analysis techniques and reporting features provided by the Cisco Firepower Management Center

Who Can Benefit

Technical professionals who need to know how to deploy and manage a Cisco Firepower NGIPS in their network environment, including:

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

Prerequisites

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

Course Details

1. Sourcefire System Overview and Classroom Setup

2. Device Management

3. Object Management

4. Access Control Policy

5. Network-based Malware Detection

6. FireSIGHT Technology

7. Correlation Policies

8. IPS Policy Basics

9. Advanced IPS Policy Configurations

10. User Account Management

11. Event Analysis

12. Reporting

13. Basic Rule Syntax and Usage

14. Case Studies in Rule Writing and Packet Analysis

Lab 1: Verifying the License

Lab 2: Testing the Environment by Running Attack PCAPs

Lab 3: Viewing Events

Lab 4: Layer 2 and 3 Simulation

Lab 5: Inline Interface Configuration

Lab 6: Creating Objects

Lab 7: Creating an Access Control Policy (Port Inspection)

Lab 8: Creating an Access Control Policy (Application Awareness)

Lab 9: URL Filtering

Lab 10: Including an IPS Policy in Access Control Rules

Lab 11: Creating a File Policy

Lab 12: Tuning the Network Discovery Policy

Lab 13: Viewing FireSIGHT Data

Lab 14: User Discovery

Lab 15: Creating a Correlation Policy Based on Connection Data

Lab 16: White Lists

Lab 17: Working with Connection Data and Traffic Profiles

Lab 18: Creating an Intrusion Policy

Lab 19: Including FireSIGHT Recommendations in an Intrusion Policy

Lab 20: Tuning Your HTTP_Inspect Preprocessor

Lab 21: Apply and Test Your Policy and Variable Set

Lab 22: Create User Accounts and Configure the UI Timeout Value

Lab 23: Testing Exempt and Non Exempt Users

Lab 24: Permission Escalation

Lab 25: Working with External Accounts

Lab 26: Analysis Lab

Lab 27: Tuning Events

Lab 28: Context Explorer

Lab 29: Comparing Trends with Reports

Lab 30: Writing Custom Rules

Lab 31: Research and Packet Analysis

Lab 32: Revisiting the Kaminsky Vulnerability