Securing Cisco Networks with Open Source Snort (SSFSNORT) v2.0

Overview
The Securing Cisco® Networks with Open Source Snort® (SSFSNORT) version 2.0 Cisco Training on Demand course provides you with technical training to successfully deploy open-source Snort technology and rule writing. Among other powerful features, you’ll learn how to build and manage a Snort system and how to update and manage rules efficiently. You’ll also learn about the Snort rules language and the capabilities of Snort when it is deployed passively and inline.

In addition, you’ll learn the requirements for installing, correctly configuring, and operating Snort. You’ll gain knowledge of the history, features, and uses of Snort, together with the public resources that are available to Snort users. Finally, the course will teach you the various output types that Snort provides, automated rule management (including how to deploy and configure Pulled Pork), inline operations, and how to create custom Snort rules, including advanced rule-writing techniques and OpenAppID.

Instructor: Ed Mendez

Duration
The SSFSNORT v2.0 Training on Demand course consists of 12 modules, totaling more than 10 hours of video instruction along with 12 hands-on lab exercises.

Read More

Target Audience
This course is designed for security administrators and consultants, network administrators, systems engineers, and technical support personnel who need to know how to deploy open-source intrusion detection systems (IDS) and intrusion prevention systems (IPS), and how to write Snort rules.

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

- Describe Snort technology and identify the resources that are available for maintaining a Snort deployment
- Install Snort on a Linux-based operating system
- Describe the Snort operation modes and their command-line options
- Describe the Snort intrusion detection output options
- Download and deploy a new rule set to Snort
- Describe and configure the snort.conf file
- Configure Snort for inline operation and configure the inline-only features
- Describe the Snort basic rule syntax and usage
- Describe how the Snort engine processes traffic
- Describe several advanced rule options used by Snort
- Describe OpenAppID features and functionality
- Describe how to monitor Snort performance and how to tune rules
Course Prerequisites
The knowledge and skills necessary before attending this course are:

- Basic understanding of networking and network protocols
- Basic knowledge of Linux command-line utilities and text-editing utilities commonly found in Linux
- Basic knowledge of network security concepts

Course Outline
- Module 1: Introduction to Snort Technology
- Module 2: Snort Installation
- Module 3: Snort Operation
- Module 4: Snort Intrusion Detection Output
- Module 5: Rule Management
- Module 6: Snort Configuration
- Module 7: Inline Operation and Configuration
- Module 8: Snort Rule Syntax and Usage
- Module 9: Traffic Flow Through Snort Rules
- Module 10: Advanced Rule Options
- Module 11: OpenAppID Detection
- Module 12: Tuning Snort

Labs Outline
This course contains 12 hands-on virtual lab exercises, powered by Cisco Learning Labs and Cisco IOS (Cisco IOS® on Linux).

Topology for All Labs in the Course:
The labs included in this course are:

- SSFSNORT2-0 Lab 1: Connecting to the Lab Environment
- SSFSNORT2-0 Lab 2: Snort Installation
- SSFSNORT2-0 Lab 3: Snort Operation
- SSFSNORT2-0 Lab 4: Snort Intrusion Detection Output
- SSFSNORT2-0 Lab 5: Pulled Pork Installation
- SSFSNORT2-0 Lab 6: Configuring Variables
- SSFSNORT2-0 Lab 7: Reviewing Preprocessor Configurations
- SSFSNORT2-0 Lab 8: Inline Operations
- SSFSNORT2-0 Lab 9: Basic Rule Syntax and Usage
- SSFSNORT2-0 Lab 10: Advanced Rules Options
- SSFSNORT2-0 Lab 11: OpenAppID
- SSFSNORT2-0 Lab 12: Tuning Snort

Instructor Bio

Ed Mendez has more than 20 years of experience as a developer and educator of course and lab content focused on a range of security products, including Checkpoint Firewall, ISS Security Suite, Snort, Cisco Firepower™, and Cisco Advanced Malware Protection. Ed is also a long-time Certified Information Systems Security Professional (CISSP), having maintained this certification for more than 14 years, and he holds product certifications in open-source Snort, Firepower, and AMP.

Cisco Capital

Financing to Help You Achieve Your Objectives

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.