

Securing Cisco Networks with Open Source Snort (SSFSNORT) v3.0

What you'll learn in this course

The **Securing Cisco Networks with Open Source Snort (SSFSNORT) v3.0** course shows you how to deploy Snort® in small to enterprise-scale implementations. You will learn how to install, configure, and operate Snort in Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) modes. You'll practice installing and configuring Snort, utilize additional software tools and define rules to configure and improve the Snort environment, and more.

Course duration

- E-learning: Equivalent of 4 days of instruction with videos, practice, and challenges

How you'll benefit

This course will help you:

- Learning how to implement Snort, an open-source, rule-based, intrusion detection and prevention system
- Gain leading-edge skills for high-demand responsibilities focused on security

Who should enroll

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

How to enroll

- For e-learning, visit the [Cisco Learning Network Store](#).
- For digital library access, visit [Cisco Platinum Learning Library](#).
- For e-learning volume discounts, contact ask_cpll@cisco.com.

Technology areas

- Security
- Cyber Operations

Course details

Objectives

After taking this course, you should be able to:

- Define the use and placement IDS/IPS components.
- Identify Snort features and requirements.
- Compile and install Snort.
- Define and use different modes of Snort.
- Install and utilize Snort supporting software.

Prerequisites

To fully benefit from this course, you should have the following knowledge and skills:

- Technical understanding of TCP/IP networking and network architecture
- Basic familiarity with firewall and IPS concepts

This is the recommended Cisco course that may help you meet these prerequisites:

- Implementing and Administering Cisco Solutions (CCNA)

Outline

- Detecting Intrusions with Snort 3.0
 - History of Snort
 - IDS
 - IPS
 - IDS vs. IPS
 - Examining Attack Vectors
 - Application vs. Service Recognition
- Sniffing the Network
 - Protocol Analyzers
 - Configuring Global Preferences
 - Capture and Display Filters
 - Capturing Packets
 - Decrypting Secure Sockets Layer (SSL) Encrypted Packets
- Architecting Nextgen Detection
 - Snort 3.0 Design
 - Modular Design Support
 - Plug Holes with Plugins
 - Process Packets
 - Detect Interesting Traffic with Rules
 - Output Data

- Choosing a Snort Platform
 - Provisioning and Placing Snort
 - Installing Snort on Linux
- Operating Snort 3.0
 - Topic 1: Start Snort
 - Monitor the System for Intrusion Attempts
 - Define Traffic to Monitor
 - Log Intrusion Attempts
 - Actions to Take When Snort Detects an Intrusion Attempt
 - License Snort and Subscriptions
- Examining Snort 3.0 Configuration
 - Introducing Key Features
 - Configure Sensors
 - Lua Configuration Wizard
- Managing Snort
 - Pulled Pork
 - Barnyard2
 - Elasticsearch, Logstash, and Kibana (ELK)
- Analyzing Rule Syntax and Usage
 - Anatomy of Snort Rules
 - Understand Rule Headers
 - Apply Rule Options
 - Shared Object Rules
 - Optimize Rules
 - Analyze Statistics
- Use Distributed Snort 3.0
 - Design a Distributed Snort System
 - Sensor Placement
 - Sensor Hardware Requirements
 - Necessary Software
 - Snort Configuration
 - Monitor with Snort
- Examining Lua
 - Introduction to Lua
 - Get Started with Lua

Lab Outline

- Capture and Analyze Packets
- Initiate the Snort Installation
- Complete an Installation of Snort
- Configure and Run Snort
- Tweak the Installation
- Rapid Deployment with Lua
- Integrate Snort Optimizers
- Analyze Rule Syntax
- Hello World Lua Style




Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

 Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Course content is dynamic and subject to change without notice.

© 2019 Cisco and/or its affiliates. All rights reserved.

SSFSNORT_3-0 C22-743093-00 11/19