Learning Services

Securing Cisco Networks with Snort Rule Writing Best Practices

Securing Cisco® Networks with Snort Rule Writing Best Practices (SSFRULES) is an instructor-led, lab-based, hands-on course offered by Cisco Learning Services. This course is part of a portfolio of security courses designed to help businesses support and maintain their Snort-based systems.

This lab-intensive course introduces you to Snort rule writing. Among other powerful features, you become familiar with:

- Snort rule development
- Snort rule language
- Standard and advanced rule options
- OpenAppID
- Tuning

The course begins by identifying the key features and characteristics of a typical Snort rule development environment. You will develop and test custom rules in a preinstalled Snort environment and identify how to use advanced rule-writing techniques. You will investigate how to include OpenAppID in your rules and also identify how to filter rules and monitor their performance.

This course combines lecture materials and hands-on labs that give you practice in creating Snort rules.

Duration

3 days
Target Audience
This course is designed for technical professionals who need to write rules for use with Snort-based intrusion detection systems (IDS) and intrusion prevention systems (IPS). The primary audience for this course includes:

- Security administrators
- Security consultants
- Network administrators
- Systems engineers
- Technical support personnel using open source IDS and IPS
- Channel partners and resellers

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

- Describe the Snort rule development process
- Describe the Snort basic rule syntax and usage
- Describe how traffic is processed by Snort
- Describe several advanced rule options used by Snort
- Describe OpenAppID features and functionality
- Describe how to monitor the performance of Snort and how to tune rules

Course Prerequisites
Cisco recommends that you have the following knowledge and skills before taking this course:

- Basic understanding of networking and network protocols
- Basic knowledge of Linux command-line utilities
- Basic knowledge of text editing utilities commonly found in Linux
- Basic knowledge of network security concepts
- Basic knowledge of a Snort-based IDS/IPS system

Course Outline
- Module 1: Introduction to Snort Rule Development
- Module 2: Snort Rule Syntax and Usage
- Module 3: Traffic Flow Through Snort Rules
- Module 4: Advanced Rule Options
- Module 5: OpenAppID Detection
- Module 6 Tuning Snort
Lab Outline

- Lab 1: Connecting to the Lab Environment
- Lab 2: Introducing Snort Rule Development
- Lab 3: Basic Rule Syntax and Usage
- Lab 4: Advanced Rule Options
- Lab 5: OpenAppID
- Lab 6: Tuning Snort

Lab Topology

Figure 1 outlines the lab topology for this course.

Registration Email

For more information about schedules and registration for this course, contact aeskt_registration@cisco.com.

Cisco Capital Financing Helps You Achieve Your Objectives

Cisco Capital® financing can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce capital expenditures (CapEx), accelerate your growth, and 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 financing is available in more than 100 countries. Learn more.
Website Addresses for More Information

For more information, visit the following websites:

- Cisco Learning Services for Cisco products and technologies: [http://www.cisco.com/go/cls](http://www.cisco.com/go/cls)