Learning Services

Securing Cisco Networks with Snort Rule Writing Best Practices (SSFRULES) v2.0

Overview
The Securing Cisco Networks with Snort Rule Writing Best Practices (SSFRULES) version 2.0 Cisco® Training on Demand course provides you with technical training in the concepts of Snort® rule development and the Snort rule language. You also learn about standard and advanced rule options, OpenAppID, and how to tune Snort rules.

In addition, you learn how to identify essential commands and supporting applications, how to examine essential components and supporting applications, the rule development process, and the format and structure of rules. You’ll gain the knowledge to understand the flow of traffic through Snort components and to explain protected content rules, byte rule options, and file detection rules. Finally, you’ll explore the OpenAppID preprocessor, events, and application detectors, and learn how to effectively read, manage, and tune Snort rules and performance.

Instructor
Ed Mendez

Duration
The SSFRULES Training on Demand course consists of 6 modules, totaling more than 7 hours of video instruction along with 6 hands-on lab exercises.

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 is security administrators, security consultants, network administrators, systems engineers, and technical support personnel using open-source IDS and IPS.
Objective

After completing this course, you should be able to:

- Describe the Snort rule development process
- Explain how traffic is processed by Snort
- Implement and configure advanced rule options used by Snort
- Understand OpenAppID features and functionality
- Monitor the performance of Snort and tune rules effectively

Course Prerequisites

The knowledge and skills necessary before attending this course is:

- Basic understanding of networking and network protocols
- Basic knowledge of command-line and 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
Labs Outline

This course contains 6 hands-on virtual lab exercises, powered by Cisco Learning Labs and Cisco IOL (Cisco IOS® on Linux).

Topology for all labs in the course:

The labs included in this course are:

- SSFRules2.0 Lab 1: Connecting to the Lab Environment
- SSFRules2.0 Lab 2: Introducing Snort Rule Development
- SSFRules2.0 Lab 3: Basic Rule Syntax and Usage
- SSFRules2.0 Lab 4: Advanced Rule Options
- SSFRules2.0 Lab 5: OpenAppID
- SSFRules2.0 Lab 6: Tuning Snort

Instructor Bio

Ed Mendez has more than 20 years of experience as an educator and developer 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 (AMP). Ed is also a long-time CISSP, having maintained this certification for more than 14 years, and he holds product certifications in open-source Snort, Cisco 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.