Training overview

Securing Cisco Networks with Snort Rule Writing Best Practices (SSFRules)

Description

The **SecuringCisco Networks with Snort Rule Writing Best Practices (SSFRules)** training shows you how to write rules for Snort, an open-source intrusion detection and prevention system. Through a combination of expert-instruction and hands-on practice, this training provides you with the knowledge and skills to develop and test custom rules, standard and advanced rules-writing techniques, integrate OpenAppID into rules, rules filtering, rules tuning, and more. The hands-on labs give you practice in creating and testing Snort rules.

This training also earns you 24 Continuing Education (CE) credits toward recertification.

How you'll benefit

This training will help you:

- Gain an understanding of characteristics of a typical Snort rule development environment
- Gain hands-on practices on creating rules for Snort
- Gain knowledge in Snort rule development, Snort rule language, standard and advanced rule options
- Earn 24 CE credits toward recertification

Who should enroll

- Security Administrators
- Security Consultants
- Network Administrators
- System Engineers
- Technical Support Personnel using open-source IDS and IPS
- Channel Partners and Resellers

Technology areas

- Security

Objectives

- 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

Prerequisites

Thereareno prerequisites for this training. However, the knowledge and skills you are recommended to have before attending this training are:

- 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

Outline

- Introduction to Snort Rule Development
- Snort Rule Syntax and Usage
- Traffic Flow Through Snort Rules
- Advanced Rule Options
- OpenAppID Detection
- Tuning Snort

Lab Outline

- Connecting to the Lab Environment
- Introducing Snort Rule Development
- Basic Rule Syntax and Usage
- Advanced Rule Options
- OpenAppID
- Tuning Snort