FIREFLY

Securing Cisco Networks with Snort Rule Writing Best Practices

DURATION: 3 DAYS COURSE CODE: SSFRULES FORMAT: LECTURE/LAB

COURSE DESCRIPTION

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 pre-installed 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.

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

WHO SHOULD ATTEND

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

LEARNING 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

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

1. Introduction to Snort Rule Development
2. Snort Rule Syntax and Usage
3. Traffic Flow Through Snort Rules
4. Advanced Rule Options
5. OpenAppID Detection
6. Tuning Snort

DISCOVERY LABS

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