FIREFLY

Securing Cisco Networks with Open Source Snort

DURATION: 4 DAYS COURSE CODE: SSFSNORT FORMAT: LECTURE/LAB

COURSE DESCRIPTION

The course begins by introducing the Snort technology and progresses through the installation and operation of Snort. You discover the various output types that Snort provides, automated rule management including how to deploy and configure Pulled Pork, inline operations, and how to create custom Snort rules, including advanced rule-writing techniques and OpenAppID.

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

This lab-intensive course introduces you to the open source Snort technology, as well as rule writing. Among other powerful features, you become familiar with:

- How to build and manage a Snort system
- How to update rules
- Snort rules language
- The capabilities of Snort when deployed passively and inline

WHO SHOULD ATTEND

This course is designed for technical professionals who need to know how to deploy open source intrusion detection systems (IDS) and intrusion prevention systems (IPS), and how to write Snort rules.

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

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

LEARNING OBJECTIVES

Describe Snort technology and identify the resources that are available for maintaining a Snort deployment

Install Snort on a Linux-based operating system

Describe the Snort operation modes and their command-line options

Describe the Snort intrusion detection output options

Download and deploy a new rule set to Snort

Describe and configure the snort.conf file

Configure Snort for inline operation and configure the inline-only features

Describe the Snort basic rule syntax and usage

Describe how traffic is processed by the Snort engine

Describe several advanced rule options used by Snort

Describe OpenAppID features and functionality

COURSE OUTLINE

1. Introduction to Snort Technology
2. Snort Installation
3. Snort Operation
4. Snort Intrusion Detection Output
5. Rule Management
6. Snort Configuration
7. Inline Operation and Configuration
8. Snort Rule Syntax and Usage
9. Traffic Flow Through Snort Rules
10. Advanced Rule Options
11. OpenAppID Detection
12. Tuning Snort

COURSE OUTLINE

1. Connecting to the Lab Environment
2. Snort Installation
3. Snort Operation
4. Snort Intrusion Detection Output
5. Unicast and Multicast RIB and FIB
6. Describing Overlay Transport Virtualization
7. Cisco OTV Overview
8. Cisco OTV Control and Data Planes
9. Failure Isolation
10. Cisco OTV Features
11. Optimizing Cisco OTV
12. Describing Virtual Extensible LAN