Securing Cisco Networks with Open Source Snort (SSFSNORT) v3.0 - On Demand

Modality: On Demand

Duration: 40 Hours

CLC: 5 Units

Course Information

About this course:

This course will teach you how to deploy Snort® in organizations of different levels ranging from small to enterprise-scale.

The course will take you through practical learning where you'll practice installing and configuring Snort, utilize additional software tools, define rules to configure and improve the Snort environment, and more. You will also learn expertise around Snort in intrusion detection system (IDS) and intrusion prevention system (IPS) modes.

Course Objective:

You will be equipped with following skill after completing this course:

- Compile and install Snort
- Define and use different modes of Snort
- Install and utilize Snort supporting software
- Define the use and placement of IDS/IPS components
- Identify Snort features and requirements

Audience:

- Network administrators
- System engineers
- Technical support personnel
- Channel partners and resellers
- Security administrators
- Security consultants

Prerequisite:

You should have the following knowledge and skills to fully benefit from this course:

- Basic familiarity with firewall and IPS concepts
- Technical understanding of TCP/IP networking and network architecture

This Cisco course is recommended to help you meet these prerequisites:

- Implementing and Administering Cisco Solutions (CCNA)

Course Outline:

Detecting Intrusions with Snort 3.0

- History of Snort
- IDS
- IPS
- IDS vs. IPS
- Examining Attack Vectors
- Application vs. Service Recognition

Sniffing the Network

- Protocol Analyzers
- Configuring Global Preferences
- Capture and Display Filters
- Capturing Packets
- Decrypting Secure Sockets Layer (SSL) Encrypted Packets

Architecting Nextgen Detection

- Snort 3.0 Design
- Modular Design Support
- Plug Holes with Plugins
- Process Packets
- Detect Interesting Traffic with Rules
- Output Data

Choosing a Snort Platform

- Provisioning and Placing Snort
- Installing Snort on Linux

Operating Snort 3.0

- Topic 1: Start Snort
- Monitor the System for Intrusion Attempts
- Define Traffic to Monitor
- Log Intrusion Attempts
- Actions to Take When Snort Detects an Intrusion Attempt
- License Snort and Subscriptions

Examining Snort 3.0 Configuration

- Introducing Key Features
- Configure Sensors
- Lua Configuration Wizard

Managing Snort

- Pulled Pork
- Barnyard2
- Elasticsearch, Logstash, and Kibana (ELK)

Analyzing Rule Syntax and Usage

- Anatomy of Snort Rules
- Understand Rule Headers
- Apply Rule Options
- Shared Object Rules
- Optimize Rules
- Analyze Statistics

Use Distributed Snort 3.0

- Design a Distributed Snort System
- Sensor Placement
- Sensor Hardware Requirements
- Necessary Software
- Snort Configuration
- Monitor with Snort

Examining Lua

- Introduction to Lua
- Get Started with Lua