Document Generated: 11/15/2024

Learning Style: On Demand

Provider: Cisco

Difficulty: Intermediate

Course Duration: 40 Hours

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

About this course:

The Securing Cisco Networks with Open Source Snort (SSFSNORT) v3.0 course shows you how to deploy Snort® in small to enterprise-scale implementations.

You will learn how to install, configure, and operate Snort in intrusion detection system (IDS) and intrusion prevention system (IPS) modes. You'll practice installing and configuring Snort, utilize additional software tools, define rules to configure and improve the Snort environment, and more.

Course Objective:

After taking this course, you should be able to:

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

Audience:

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

Prerequisite:

To fully benefit from this course, you should have the following knowledge and skills:

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

This is the recommended Cisco course that may 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

Credly Badge:

Display your Completion Badge And Get The Recognition You Deserve.

Add a completion and readiness badge to your Linkedin profile, Facebook page, or Twitter account to validate your professional and technical expertise. With badges issued and validated by Credly, you can:

- Let anyone verify your completion and achievement by clicking on the badge
- Display your hard work and validate your expertise
- Display each badge's details about specific skills you developed.

Badges are issued by QuickStart and verified through Credly.

Find Out More or See List Of Badges