Securing Cisco Networks with Open Source Snort

Duration: 4 Days **Course Code: SSFSNORT** **Version: 2.1**

Overview:

The Securing Cisco Networks with Open Source Snort course shows you how to deploy a network intrusion detection system based on Snort. Through a combination of expert instruction and hands-on practice, you will learn how to install, configure, operate, and manage a Snort system, rules writing with an overview of basic options, advanced rules writing, how to configure PulledPork, and how to use OpenAppID to provide protection of your network from malware. You will learn techniques of tuning and performance monitoring, traffic flow through Snort rules, and more.

This course is worth 32 Continuing Education (CE) Credits

Target Audience:

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 write Snort rules.

Objectives:

- **After completing this course, you should be able to:**
- 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 command-line options for starting SNORT as a sniffer, as a logger, and as an intrusion detector, and create a script to start Snort automatically.
- Describe the Snort operation modes and their command-line options.
- Describe Snort intrusion detection outputs.
- Describe rule sources, updates and utlilties for managing rules and updates.
- Describe and configure the snort.conf file.
- Describe how to configure Snort for inline operation using the inline-only features.
- Describe the Snort basic rule syntax and usage.
- Describe how traffic flows through Snort and how to optimze rules for better performance.
- Describe advanced rule writing features of Snort.
- Describe OpenAppID features and functionality.
- Describe Tuning Snort.

Prerequisites:

Attendees should meet the following prerequisites:

- Technical understanding of TCP/IP networking and network architecture
- Proficiency with Linux and UNIX text editing tools (vi editor is suggested but not required)

Testing and Certification

Recommended as preparation for exams:

- There are no exams currently aligned to this course

Content:

Introducing Snort Technology

- Snort Basics
- Snort Resources

Installing Snort

- Installation Prerequisites
- Performing the Snort Installation

Introducing Snort Operations

- Running Snort from the Command Line
- Configuring Snort to Start Automatically

Understanding Snort Intrusion Detection Output

- Configuring Snort Intrusion Detection Output
- Processing Unified2 Output with Banyard2

Understanding Rule Management

- Snort Rule Sets
- PulledPork Installation and Configuration

Understanding Snort Configuration

- Examining the snort.conf file sections
- Preprocessor Configuration

Understanding Inline Operation and Configuration

- Configuring Inline Operation
- Configuring Inline-Specific Features

Understanding Snort Rule Syntax and Usage

- Basic Rule Syntax
- Common Rule Options

Understanding Traffic Flow Through Snort Rules

- Examining Snort Traffic Flow

Examining Advanced Rule Options

- PCRE Rule Options
- Protected Content Rules
- Byte Rule Options
- Implementing Flowbits
- File Detention

Configuring OpenAppID Detection

- Exploring the Open AppID Preprocessor
- Examining AppID Events and Statistics
- Examining Application Detectors

Tuning Snort

- Viewing Performance Statistics
- Configuring Snort Rule Filters
- Implementing BPFs in Snort
- Performance Profiling

Labs

- Lab 1: Connecting to the Lab Environment
- Lab 2: Snort Installation
- Lab 3: Snort Operation
- Lab 4: Snort Intrusion Detection Output
- Lab 5: PulledPork Installation
- Lab 6: Configuring Variables
- Lab 7: Reviewing Preprocessor Configurations
- Lab 8: Inline Operations
- Lab 9: Basic Rule Syntax and Usage
- Lab 10: Advanced Rule Options
- Lab 11: OpenAppID
- Lab 12: Tuning Snort

Further Information:

For More information, or to book your course, please call us on 0800/84.009

info@globalknowledge.be

www.globalknowledge.com/en-be/