Securing Cisco Networks with Open Source Snort

Duration: 4 Days   **Course Code: SSFSNORT**   **Version: 2.1**   **Delivery Method: Virtual Learning**

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 Pulled Pork, 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.

Virtual Learning

This interactive training can be taken from any location, your office or home and is delivered by a trainer. This training does not have any delegates in the class with the instructor, since all delegates are virtually connected. Virtual delegates do not travel to this course, Global Knowledge will send you all the information needed before the start of the course and you can test the logins.

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 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

■ Describe how to monitor of Snort performance and how to tune rules

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:

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

- Lab 1: Connecting to the Lab Environment
- Lab 2: Snort Installation
- Lab 3: Snort Operation
- Lab 4: Snort Intrusion Detection Output
- Lab 5: Pulled Pork 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 Head Office 01189 123456 / Northern Office 0113 242 5931

info@globalknowledge.co.uk

www.globalknowledge.com/en-gb/

Global Knowledge, Mulberry Business Park, Fishponds Road, Wokingham Berkshire RG41 2GY UK