Securing Cisco Networks with Open Source Snort (SSFSNORT)

Duration 4 Days

COURSE CONTENT

Securing Cisco® Networks with Open Source SnortTM (SSFSNORT) is an instructor-led course offered by Cisco Learning Services High-Touch Delivery. It is a lab-intensive course that introduces students to the open source Snort technology as well as rule writing. You will learn how to build and manage a Snort system using open source tools, plug-ins, and the Snort rule language to help manage, tune, and deliver feedback about suspicious network activity. This course combines lecture materials and hands-on labs throughout to make sure that you are able to construct a solid, secure Snort installation and write Snort rules using proper syntax and structure. This course prepares you to take the Securing Cisco Networks with Open Source Snort exam (exam ID 500-280).

COURSE OUTLINE

- **Module 1:** Intrusion Sensing technology, Challenges, and Sensor Deployment
- **Module 2:** Introduction to Snort Technology
- **Module 3:** Snort Installation
- **Module 4:** Configuring Snort for Database Output and Graphical Analysis
- **Module 5:** Operating Snort
- **Module 6:** Snort Configuration
- **Module 7:** Configuring Snort Preprocessors
- **Module 8:** Keeping Rules Up-to-date
- **Module 9:** Building a Distributed Snort Installation
- **Module 10:** Basic Rule Syntax and Usage
- **Module 11:** Building a Snort IPS Installation
- **Module 12:** Rule Optimization
- **Module 13:** Using Perl Compatible Regular Expressions (PCRE) in Rules
- **Module 14:** Basic Snort Tuning
- **Module 15:** Using Byte_Jump, Byte_Test and Byte_Extract Rule Options
- **Module 16:** Protocol Modeling Concepts and Using Flowbits in Rule Writing
- **Module 17:** Case Studies in Rule Writing and Packet Analysis

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), as well as write Snort rules. The primary audience for this course includes: Security administrators Security consultants Network administrators System engineer Technical support personnel using open source IDS and IPS Channel partners and resellers

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)

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th
Call us today 0-2634-7993-4
177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th