SECURING CISCO NETWORKS WITH OPEN SOURCE SNORT

DURATION: 4 DAYS

COURSE OVERVIEW

Securing Cisco Networks with Open Source Snort 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 on 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.

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.

COURSE OBJECTIVES

After completing this course, you should be able to:

1. Understand what Snort is and its basic architectural components
2. Understand Snort's dynamic plug-in capabilities
3. Understand the different modes of Snort operation
4. Perform installation and configuration of the Snort system
5. Install and configure Snorby
6. Configure and tune the Snort pre-processors
7. Understand rule maintenance and techniques to keep rules current
8. Create Snort rules using both simple and advanced rule-writing techniques
9. Monitor performance of a Snort deployment

COURSE CONTENT

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 Pre processors

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 PCRE in Rules

Module 14: Basic Snort Tuning

Module 15: Using Byte Jump/Test/Extract Rule Options

Module 16: Protocol Modeling Concepts and Using Flow bits in Rule Writing

Module 17: Case Studies in Rule Writing and Packet Analysis

Labs

Lab 1: Install Snort and Its Components (Module 3)
Lab 2: Barnyard2 Installation (Module 4)
Lab 3: Barnyard and Snorby Configuration (Module 4)
Lab 4: Operating Snort (Module 5)
Lab 5: Configuring Your IDS/IPS Installation (Module 6)
Lab 6: Port scan Configuration (Module 7)
Lab 7: Stream Reassembly (Module 7)
Lab 8: Pulled Pork Installation, Configuration, and Usage (Module 8)

Lab 9: Building a Distributed Snort Installation (Module 9)

Lab 10: Weighting Custom Rules (Module 10)

Lab 11: Building an Inline IPS (Module 11)

Lab 12: Using the Drop Action (Module 11)

Lab 13: Using the Replace Action (Module 11)

Lab 14: Optimizing Rules (Module 12)

Lab 15: Using and Testing PCRE in Rules (Module 13)

Lab 16: Using Event Filtering (Module 14)

Lab 17: Using Suppression (Module 14)

Lab 18: Configuring Rule Profiling (Module 14)

Lab 19: Detecting SADMIND Trust with Byte Jump and Byte Test (Module 15)

Lab 20: Using the Bitwise AND Operation in Byte Test (Module 15)

Lab 21: Detecting Zen Works Directory Traversal with Byte Extract (Module 15)

Lab 22: Writing Flow bits Rules (Module 16)

Lab 23: Research and Packet Analysis (Module 17)

Lab 24: Revisiting the Kaminsky Vulnerability (Module 17)

COURSE PREREQUISITES

Attendees should meet the following prerequisites:

Technical understanding of TCP/IP networking and network architecture - ICND1 recommended

Proficiency with Linux and UNIX text editing tools (vi editor is suggested but not required)