SECURING CISCO NETWORKS WITH SNORT RULE WRITING BEST PRACTICES

DURATION: 3 DAYS

COURSE OVERVIEW

Securing Cisco Networks with Snort Rule Writing Best Practices is a lab-intensive course that introduces students to the open source Snort community and rule-writing best practices. Users focus exclusively on the Snort rules language and rule writing. Starting from rule syntax and structure to advanced rule-option usage, you will analyze exploit packet captures and put the rule writing theories learned to work—implementing rule-language features to trigger alerts on the offending network traffic. This course also provides instruction and lab exercises on how to detect certain types of attacks, such as buffer overflows, utilizing various rule-writing techniques. You will test your rule-writing skills in two challenges: a theoretical challenge that tests knowledge of rule syntax and usage, and a practical challenge in which we present an exploit for you to analyze and research so you can defend your installations against the attack. This course combines lecture materials and hands-on labs throughout to make sure that you are able to successfully understand and implement open source rules.

TARGET AUDIENCE

This course is designed for:

Security professionals who need to know how to write rules and understand open source Snort language.

COURSE OBJECTIVES

After completing this course, you should be able to:

1. Understand rule structure, rule syntax, rule options, and their usage
2. Configure and create Snort rules
3. Understand the rule optimization process to create efficient rules
4. Understand preprocessors and how data is presented to the rule engine
5. Create and implement functional Regular Expressions in Snort rules
6. Design and apply rules using byte jump/test/extract rule options
7. Understand the concepts behind protocol modeling to write rules that perform better

COURSE CONTENT

Module 1: Welcome to the Sourcefire Virtual Network

Module 2: Basic Rule Syntax and Usage

Module 3: Rule Optimization

Module 4: Using PCRE in Rules

Module 5: Using Byte Jump/Test/Extract Rule Options

Module 6: Protocol Modeling Concepts and Using Flow bits in Rule Writing

Module 7: Case Studies in Rule Writing and Packet Analysis

Module 8: Rule Performance Monitoring

Module 9: Rule Writing Practical Labs, Exercises, and Challenges

Labs

Lab 1: Writing Custom Rules
Lab 2: Drop Rules
Lab 3: Replacing Content
Lab 4: SSH Rule Scenerio
Lab 5: Optimizing Rules
Lab 6: Using PCR Etest to Test Regex Options
Lab 7:Use PCR Etest to Test Custom Regular Expressions
Lab 8: Writing Rules That Contain PCRE
Lab 9: Detecting SADMIND Trust with Byte Jump and Byte test
Lab 10: Using the Bitwise AND Operation in Byte Test Rule Option
Lab 11: Detecting Zen Works Directory Traversal Using Byte Extract
Lab 12: Writing a Flow bit Rule
Lab 13: Extra Flow bits Challenge
Lab 14: Strengthen Your Brute-Force Rule with Flow bits
Lab 15: Research and Packet Analysis
Lab 16: Revisiting the Kaminsky Vulnerability
Lab 17: Configuring Rule Profiling
Lab 18: Testing Rule Performance
Lab 19: Configure Rule Profiling to View PCRE Performance
Lab 20: Preventing User Access to a Restricted Site
Lab 21: SQL Injection
Lab 22: The SQL Attack Revisited

COURSE PREREQUISITES

Attendees should meet the following prerequisites:

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

Working knowledge of how to use and operate Cisco Sourcefire Systems or open source Snort

Working knowledge of command-line text editing tools, such as the vi editor

Basic rule-writing experience is suggested