
Securing Cisco Networks with Snort Rule Writing Best Practices

Duration: 3 Days Course Code: SSFRULES

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.

Objectives:

- | | |
|---|---|
| <ul style="list-style-type: none">■ After completing this course, you should be able to:■ Understand rule structure, rule syntax, rule options, and their usage■ Configure and create Snort rules■ Understand the rule optimization process to create efficient rules | <ul style="list-style-type: none">■ Understand preprocessors and how data is presented to the rule engine■ Create and implement functional Regular Expressions in Snort rules■ Design and apply rules using byte_jump/test/extract rule options■ Understand the concepts behind protocol modeling to write rules that perform better |
|---|---|
-

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
-

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 Flowbits 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 PCREtest to Test Regex Options
- Lab 7: Use PCREtest 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 ZenWorks Directory Traversal Using Byte_Extract
- Lab 12: Writing a Flowbit Rule
- Lab 13: Extra Flowbits Challenge
- Lab 14: Strengthen Your Brute-Force Rule with Flowbits
- 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

Further Information:

For More information, or to book your course, please call us on 353-1-814 8200

info@globalknowledge.ie

www.globalknowledge.com/en-ie/

Global Knowledge, 3rd Floor Jervis House, Millennium Walkway, Dublin 1