Securing Cisco Networks with Snort Rule Writing Best Practices

Duration: 3 Days **Course Code: SSFRULES** **Version: 2.1**

Overview:

Securing Cisco Networks with Snort Rule Writing Best Practices is a lab-intensive course that introduces users of open source Snort or Sourcegire FIRESIGHT systems to the Snort rules language 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:

- **After completing this course, you should be able to:**
- Describe rule structure, rule syntax, rule options and their usage.
- Configure and create Snort rules
- Describe the rule optimization process to create efficient rules
- Describe 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

Testing and Certification

Recommended as preparation for exams:

- There are no exams currently aligned to this course

Content:

Module 1: Welcome to the Cisco and Sourcefire Virtual Network

Module 2: Basic Rule Syntax and Usage

Module 3: Rule Optimization

Module 4: Using Perl Compatible Regular Expressions (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 Sudies in Rule Writing and Packet Analysis

Module 8: Rule Performance Monitoring

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

Labs

- Lab 1: Infrastructure Familarization
- Lab 2: Writing Custom Rules
- Lab 3: Drop Rules
- Lab 4: Replacing Content
- Lab 5: SSH Rule Scenerio
- Lab 6: Optimizing Rules
- Lab 7: Using PCREtest to Test Regex Options
- Lab 8: Use PCREtest to Test Custom Regular Expressions
- Lab 9: Writing Rules That Contain PCRE
- Lab 10: Exploiting SADMIND Trust
- Lab 11: Using the Bitwise AND Operation in Byte_Test Rule Option
- Lab 12: Detecting ZenWorks Directory Traversal Using Byte_Extract
- Lab 13: Writing a Flowbit Rule
- Lab 14: Extra Flowbits Challenge
- Lab 15: Strengthen Your Brute-Force Rule with Flowbits
- Lab 16: Research and Packet Analysis
- Lab 17: Revisiting the Kaminsky Vulnerability
- Lab 18: Configuring Rule Profiling
- Lab 19: Testing Rule Performance
- Lab 20: Configure Rule Profiling to View PCRE Performance
- Lab 21: Preventing User Access to a Restricted Site
- Lab 22: SQL Injection
- Lab 23: The SQL Attack Revisited

Further Information:

For More information, or to book your course, please call us on 0800/84.009

info@globalknowledge.be

www.globalknowledge.com/en-be/