Securing Cisco Networks with Snort Rule Writing Best Practices (SSFRULES)

Duration 3 Days

COURSE CONTENT

Securing Cisco® Networks with Snort Rule Writing Best Practices (SSFRULES) is an instructor-led course offered by Cisco Learning Services High-Touch Delivery. It's a lab-intensive course that introduces users of open source Snort or Sourcefire FireSIGHT1 systems to the Snort rules language and rule-writing best practices. You will 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 by 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, using various rule writing techniques. You will test your rule writing skills with two challenges: a theoretical challenge that tests your knowledge of rule syntax and usage, and a practical challenge in which you analyze and research an exploiting event, so you can defend your installations against attacks 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.

COURSE OUTLINE

- **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, Byte_Test and Byte_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 Practical Labs, Exercises, and Challenges

WHO SHOULD ATTEND

This course is designed for technical professionals who need to know how to write rules and understand open source Snort language.

The primary audience for this course includes:

- Security administrators
- Security consultants
- Network administrators
- System engineers
- Technical support personnel
- Channel partners and resellers

PREREQUISITES

Technical understanding of TCP/IP networking and network architecture

- Working knowledge of how to use and operate Cisco and 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

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