Preparation Securing Cisco Networks with Snort Rule Writing Best Practices

This course is 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. It 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.

Who Needs to Attend

- Security Administrators
- Security Consultant s
- Network Administrators
- System Engineers
- Technical Support Personnel
- Channel Partners and Resellers

Course Certifications

This course is part of the following Certifications:

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

Course Objectives

- Describe Snort rules language and rule writing
- Describe rule syntax and structure to advance rule option usage
- 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

Course Content

Module 1: Introduction to Snort Rule Development

Module 2: Snort Rule Syntax and Usage

Module 3: Traffic Flow Through Snort Rules

Module 4: Advanced Rule Options

Module 5: OpenAppID Detection

Module 6: Tuning Snort