Securing Cisco Networks with Snort Rule Writing Best Practices (SSFRules) Training

Duration: **3 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

The Securing Cisco Networks with Snort Rule Writing Best Practices (SSFRules) v2.1 course shows you how to write rules for Snort, an open-source intrusion detection and prevention system. Through a combination of expert-instruction and hands-on practice, this course provides you with the knowledge and skills to develop and test custom rules, standard and advanced rules-writing techniques, how to integrate OpenAppID into rules, rules filtering, rules tuning, and more. The hands-on labs give you practice in creating and testing Snort rules.

This course will help you:

- Gain an understanding of characteristics of a typical Snort rule development environment
- Gain hands-on practices on creating rules for Snort
- Gain knowledge in Snort rule development, Snort rule language, standard and advanced rule options

Prerequisites

To fully benefit from this course, you should have:

- Basic understanding of networking and network protocols
- Basic knowledge of Linux command-line utilities
- Basic knowledge of text editing utilities commonly found in Linux
- Basic knowledge of network security concepts
- Basic knowledge of a Snort-based IDS/IPS system

What You Will Learn

After taking this course, you should be able to:

- Describe the Snort rule development process
- Describe the Snort basic rule syntax and usage
- Describe how traffic is processed by Snort
- Describe several advanced rule options used by Snort
- Describe OpenAppID features and functionality
- Describe how to monitor the performance of Snort and how to tune rules