

Course Description: This two-day class provides an in-depth look at Snort rules and Snort rules language syntax. Snort is the most widely used open source Intrusion Detection product. Learning how to take advantage of the power behind Snort rules can help security administrators write and configure highly effective rules. This class features extensive hands-on rules development and testing to reinforce the theoretical concepts that are presented.

Who Should Attend: Network Administrators, security administrators, security consultants and those that are responsible for deploying open source Intrusion Detection sensors in their organizations.

Prerequisites: This course assumes that students have a technical understanding of TCP/IP networking and network architecture. Proficiency with Linux and UNIX text editing tools (vi editor) is suggested, not required.

Benefits of Attendance: Upon completion of this course, students will be able to:

- Write and configure highly effective rules
- Understand Snort rules and Snort rules language syntax
- Apply good rule writing practices
- Using advanced rule syntax

Course Outline:

Introduction

Rule management

Variables

Anatomy of a Snort rule

Good rule writing practices

Using advanced rule syntax

Using PCRE in Snort Rules

Testing rules

Tuning rules

Rule & Preprocessor Profiling