

Course Description: This two-day class is for those who want to learn how to build a Snort IDS/IPS from scratch using many of the open source tools and plug-ins available to help manage, tune and deliver feedback on suspicious activity in your networks. Hands-on labs with fully documented instructions help students construct solid, secure Snort installations and understand the inner workings of the premier open source IDS/IPS available today. Students will also learn how to fine tune and configure Snort in addition to creating custom rules and learning techniques for optimizing rules.

Who Should Attend: Network Administrators, security administrators, security consultants and others 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:

- Build a Snort IDS/IPS from scratch
- Construct solid, secure Snort installations
- Understand the inner workings of the premier open source IDS/IPS available today.
- Fine tune and configure Snort
- Create custom rules and learning techniques for optimizing rules

Course Outline:

Introduction to Snort

Snort Architecture

Snort Sensor Deployment

Snort Installation

Snort Configuration and Operation

Snort Rules Primer

Snort Preprocessor Operation

Snort Tuning

Snort Output Processing