CISCO TRAINING

Securing Cisco Networks with Open Source Snort

Secure your Cisco networks with Open Source Snort. Master intrusion detection and analysis to protect against cyber threats.

DURATION
2 hours

LEVEL
Intermediate

FORMAT
Instructor-Led

- Globally Recognized Certification
- Expert-Led Hands-On Training
- Flexible Scheduling

Computer Pride | 1st Floor, ICEA Building, Kenyatta Avenue, Nairobi | www.computer-pride.co.ke

COURSE OVERVIEW

This intermediate-level course, "Securing Cisco Networks with Open Source Snort," provides an in-depth exploration of leveraging the powerful open-source intrusion detection/prevention system (IDS/IPS), Snort, to fortify Cisco network infrastructures. Participants will learn how to deploy, configure, and manage Snort effectively to detect and prevent a wide range of cyber threats, from malware and exploits to policy violations, specifically within environments protected by Cisco networking equipment. The curriculum emphasizes practical application, allowing learners to gain hands-on experience in real-world scenarios.

By the end of this 2-hour intensive course, you will possess the critical skills to enhance your organization's security posture by integrating Snort into existing Cisco security frameworks. This includes mastering Snort rule creation, understanding alert mechanisms, and interpreting security events to respond proactively to threats. This specialized knowledge is invaluable for IT professionals looking to advance their capabilities in network security, offering a distinct advantage in safeguarding complex network environments and ensuring business continuity against evolving cyber threats.

Duration	2 hours
Level	Intermediate
Vendor	Cisco

COURSE CURRICULUM

01 Module 1: Introduction to Network Intrusion Detection and Snort Fundamentals

- Overview of Intrusion Detection/Prevention Systems (IDS/IPS)
- Key concepts of network security monitoring
- Introduction to Snort: Architecture, components, and modes of operation
- Setting up a Snort environment on a Linux platform
- Basic Snort command-line usage and initial configuration

02 Module 2: Understanding and Writing Snort Rules

- Snort rule syntax: header and options
- Common rule keywords and their usage (e.g., content, sid, rev)
- Writing custom Snort rules for specific threat detection
- Testing and validating Snort rules for effectiveness
- Performance considerations when writing rules

03 Module 3: Integrating Snort with Cisco Network Devices

- Strategies for deploying Snort within a Cisco-centric network topology
- Configuring SPAN/RSPAN ports on Cisco switches for traffic mirroring
- Best practices for sensor placement in a Cisco environment
- Understanding network traffic flows in Cisco networks for optimal Snort deployment
- Initial alert correlation between Snort and Cisco device logs

04 Module 4: Snort Alerting, Logging, and Analysis

- Understanding Snort output formats (unified2, text, database)
- Configuring alert destinations and logging mechanisms
- Analyzing Snort alerts using command-line tools
- Introduction to Snort reporting and visualization tools (e.g., Snorby, BASE)
- Developing incident response procedures based on Snort detections

CAREER PATHWAYS

Graduates of this program are prepared for the following roles:

> **Network Security Analyst specializing in IDS/IPS Operations**

> **Security Operations Center (SOC) Tier 2 Analyst with Cisco & Snort Expertise**

> **Cybersecurity Consultant focusing on Network Intrusion Detection**

FREQUENTLY ASKED QUESTIONS

Q: What specific skills will I gain that are directly applicable to securing Cisco networks?

This course will equip you with the practical skills to configure Snort sensors to monitor traffic on Cisco-powered networks, write custom Snort rules tailored to your organization's specific Cisco environment, and interpret Snort alerts to identify and respond to threats targeting Cisco infrastructure. You will learn to integrate Snort's capabilities with your existing Cisco security operations.

Q: Are there any specific prerequisites or prior knowledge recommended for this course beyond the 'Intermediate' level?

While listed as Intermediate, it is highly recommended that participants have a foundational understanding of networking concepts (TCP/IP, common protocols), basic Linux command-line proficiency, and some familiarity with Cisco networking devices and their basic configuration. Experience with network security concepts or other security tools would also be beneficial but is not strictly required.

Q: How does learning Open Source Snort benefit my career if I primarily work with Cisco's proprietary security solutions like Firepower IDS/IPS?

Mastering Snort provides a versatile and cost-effective skill set that complements proprietary solutions. Many Cisco Firepower appliances actually leverage Snort rules internally, making your understanding of Snort syntax and logic directly transferable. Furthermore, knowing Snort allows you to build custom detections for unique threats that might not be covered by commercial signatures, enhancing your overall ability to secure diverse network environments and differentiate your expertise.

ABOUT COMPUTER PRIDE

East Africa's Premier IT Training Center

With over 15 years of excellence, Computer Pride delivers globally recognized certification programs from leading technology vendors. Located on Kenyatta Avenue in Nairobi's CBD, our state-of-the-art facilities and expert instructors have empowered thousands of professionals across East Africa.

15+	10,000+	50+
Years of Excellence	Professionals Trained	Vendor Certifications

READY TO ENROL?

Take the next step in your technology career.

Location
1st Flr, ICEA Building
Kenyatta Ave, Nairobi

Email
info@computer-pride.co.ke

Phone
+254 705 900 900

www.computer-pride.co.ke