Open Source Security Tools

5 Days

Open Source Security Tools is a five-day hands-on course that eliminates the need for you to research and test the broad range of open source tools in search of what works best.

At VeriSign, we provide the best-of-breed tools to you, teach you how to effectively use them in our labs, and provide the confidence to implement them in your specific network environment.

Most enterprises have made a significant investment in a robust, commercial firewall product to protect their perimeter. At the same time, many enterprises overlook some critical elements of a comprehensive network security strategy, including assessment testing, intrusion detection, and studying network traffic.

VeriSign has identified more than a dozen open source tools—which our security consultants have successfully used in hundreds of large and small-scale networks—to help you round out your network security implementation.

We have done extensive research and testing on these tools, and now have created a training course that gives you the knowledge and skills to quickly and effectively identify and repair vulnerabilities in your network.

What You Will Learn:
The goal of the Open Source Security Tools course is to develop security awareness among students and enable them to implement a security strategy utilizing open source solutions to solve technical security problems.

The categories of tools and techniques presented include:

- OS Hardening Techniques
- Open Source Sniffers
- Open Source Scanners
- Open Source Secure Communications Protocols and Applications
- Open Source Firewalls
- Open Source Intrusion Detection Systems
- Open Source Log and System Maintenance tools

Who Should Attend:
This course is designed for IT professionals responsible for:

- Organizational and Enterprise security
- System Administration
- Network Administration

Open Source Security Tools Course Outline

Chapter 1: Open Source and Technology Review

This is a comprehensive overview of open source technology with emphasis on handling open source tools for implementation. You'll learn tips, tricks and techniques for validating, compiling and using open source tools.

- An introduction to Open Source Technology
- File and system utilities for handling open source
- Implementation considerations

Chapter 2: Operating System Hardening

This is a detailed lecture and lab chapter, which teaches operating system hardening techniques to eliminate vulnerabilities. You will apply what you learn in this section and create a secure operating system for use in the remainder of the course.

Techniques presented include: OS Hardening, testing and verification

Chapter 3: Scanners

This is a detailed lecture and lab chapter, which introduces Open Source Scanners as a means of determining your system vulnerabilities. In this chapter you will learn how to install, configure and operate scanners and analyze the scanner output.

Scanners included in this section are NMap, Whisker, Satan, Santa, Saint, Nessus

Chapter 4: Sniffers

This is a detailed lecture and lab chapter, which introduces Open Source Sniffers as a means of capturing data, and detecting unauthorized sniffers in use on your network. In this chapter you will learn how to install, configure and operate sniffers and analyze their output.

Sniffers included in this section are Ethereal, dSniff, SSLDump

Chapter 5: Secure Communications

This is a detailed lecture and lab chapter, which introduces Open Source Secure Communications tools and techniques as a means of protecting network traffic. In this chapter you will learn to implement these techniques and tools and analyze their effectiveness.

Tools included in this section are: OpenSSL, Stunnel, OpenSSH, VNC, FreeSWANSFTP

Chapter 6: Fire Walls

This is a detailed lecture and lab chapter, which introduces Open Source Fire Walls as a means of providing perimeter security in your network environment.

In this chapter you will install, configure and implement an open source firewall and test it for effectiveness.

Firewalls included in this section are: ipchains, netfilter, tcp wrappers, Iptables, and Firebox II

Chapter 7: Intrusion Detection Systems

This is a detailed lecture and lab chapter, which introduces Open Source Intrusion Detection Systems as a means of detecting unauthorized network activities. In this chapter you will learn to install, configure and operate IDS's and how to evaluate their effectiveness in your environment.

The primary IDS's presented in this chapter are: Snort, Shadow and Tripwire

Chapter 8: Log and System Administration (Maintenance)

This is a detailed lecture and lab chapter, which introduces Open Source Log Maintenance Tools and techniques for analyzing system logs. In this chapter you will learn to install, configure and operate several log and maintenance tools for the purpose of identifying unauthorized activities.

Tools included in this chapter are: Nannie, Wtmp, FTP Logger, http-analyze, LogCheck and NetLog

> *"I was amazed by the chapter on sniffers, and equally jazzed by the section on secure communications."*
>
> \- **Beth Milliken, Abuse Engineer, Earthlink/MindSpring**

To register, visit: www.verisign.com/learn
To schedule Onsite training call 650-426-5310.