

Course 622: Securing Linux (5 Days)

Course Description...

Security Linux is the first course in ROI Training's Linux Security curriculum. This hands-on intensive workshop focuses on hardening the Linux system. The course starts with methods for auditing a production system and then moves on to the tools necessary for continuous security monitoring. The course covers IPtables, SELinux, PAM, and Kerberos in depth. Methods of protecting the network including IDS are covered. The course covers theory only when it will enhance understanding of the tools and techniques being used. Approximately 80% of the class time is hands-on configuration and testing using Red Hat 5.3.

Suggested Prerequisites...

To receive the maximum benefit from this course attendees should have a background equivalent to that provided by ROI's *Linux Workstation: Installing, Customizing, and Securing* course (#603).

Who should attend...

Linux system administrators, network administrator who have Linux hosts on the network, programmers working on Linux projects, system architects who need to target Linux hosts, anyone wanting a technical knowledge of the mechanism used to secure a Linux host.

Learning Objectives...

- How to perform a security audit
- How to harden the boot sequence, login and gnome
- How to monitor the system
- How to use kerberos for better security
- How PAM works and how to use it
- Understand and build Red Hat IPtables and advanced IPtables
- How to use SELinux
- How to use Kerberos
- Know how to use the methods of protecting data on a disk
- Know how to setup ssh with

See next page for a detailed course outline...



Course Outline...

Introduction and Overview

Course Objectives

How to use the course materials to harden a Linux system

Unit 1 – Auditing a Production System

- Using checklists
- Scanning for exploits and root kits
- Testing passwords
- Testing access with nmap and Nessus
- Managing SUID/SGID programs
- Checking services
- Checking other programs
- Bastille and other automated systems

Unit 2 – Monitoring the System

- Monitoring system resources
- Monitoring in the kernel
- Monitoring network connections
- Monitoring log files
- A replacement for syslog

Unit 3 – Booting and init

- BIOS and grub security
- Virtual terminals and other init actions
- Login screen changes
- Daemon management

Unit 4 – General Network Changes

- Closing ports
- xinetd services
- Limiting access

Unit 5 – Intrusion Detection

- Simple rpm checks
- After the fact with AIDE or Tripwire
- Using an IDS

Unit 6 – IPtables

- IPtables tutorial
- Red Hat's IPtables
- Advanced configuration of IPtables

Unit 7 – SELinux

- SELinux tutorial
- Type enforcement
- Users and Roles
- Security Policy
- Managing SELinux



Unit 8 – Kerberos

- Kerberos tutorial
- Identification
- Securing resources

Unit 9 – PAM

- PAM tutorial
- Setting limits
- Restricting su
- Password management
- Interactions with Kerberos

Unit 10 – Disk Security

- The kinds of ACLs
- File Attributes
- Limiting capabilities with ICAP
- Limiting root's capabilities
- Encrypting files
- Disk encryption

Unit 11 – Tuneable Parameters

- CPU
- Memory
- Network

Unit 12 – Secure Services

- The ssh family of commands with public key encryption
- nfs4 with ACLs

Please contact your ROI representative to discuss tailoring/customizing this course to your environment!!!