

Control and Security of Linux

Course Duration:	2 Days
CPE Hours:	16 Hours
Level:	Intermediate/Group-Live
Prerequisites:	None
Advanced Preparation:	None

Linux has quickly become a major player in the world of operating systems. Businesses are looking for lower-cost alternatives to Windows and UNIX while meeting the increased demands for accessibility, functionality, scalability and reliability while maintaining a high level of security. Linux runs on all types of machines from PDA's to IBM mainframes. This versatile operating system can be used to host almost any business process from network routing and workstation operations to Internet e-commerce servers, or even as a firewall. Linux offers a plethora of security features that, when properly adapted and configured, provide the security needed for both commercial and government requirements. This seminar will provide the participants with a working knowledge of the controls available in the Linux environment and how to manage and monitor those controls. Each participant will receive a copy of the Canaudit Linux Audit Script, which is a valuable tool for assessing Linux security. They will also receive a copy of the Canaudit Linux Audit and Security Guide. This guide contains a full set of the Canaudit Linux Security Risk/Control Tables and our comprehensive Audit and Security Checklists.

Who Should Attend:

This seminar is intended for IT Security professionals and auditors who will be conducting Linux security reviews. It is also useful for business managers and entry-level system administrators who want to build and maintain secure Linux systems. A basic understanding and experience with Linux are required.

Seminar Outline:

I. Understanding Linux

II. Secure Linux Installation

- Secure partitioning for Linux
- System BIOS considerations
- Linux boot loaders
 - GRUB vs. LILO
 - Single-user mode
- Package selection and installation
- Authentication
- The basic Linux file structure
- The X Window System
- Developing standardized builds
- Linux security baselines
 - Tripwire

III. General Linux Security

- Security policy and physical security
- User awareness and training
- Backup and recovery
- File encryption
- Linux files
 - Permissions
 - Linux file attributes
 - Linux file types
 - Sticky bits
- Logging via syslogd
- Warning banners

IV. Linux Account and Password Management

- Account administration
- Group administration
- Password security controls
- PAM
- Linux account and password auditing (cracking)

V. Hardening the Linux Operating System

- Restricting remote access services
 - SSH vs. simple services
 - TCP wrappers
 - xinetd and inetd
 - Chroot jail environment
- Protecting superuser
 - set-UID and set-GID
 - SU and SUDO
 - Remote root access
- Bastille Linux for hardening
- Linux packet-filtering firewalls
 - Netfilter and Lptables

VI. Linux Audit and Assessment

- Conducting Linux-based risk assessments
- Vulnerability assessments
- Penetration testing
- Linux security audit tools
 - LSAT, CIS scoring tool and Bastille assessment
 - NMap and Nessus

VII. Secure Linux Administration

- Patching and upgrading
- Security monitoring
- Cron, at and batch scheduling
- Resource management

VIII. Common Linux Vulnerabilities and Exploit Techniques

- Root kits
- Service exploits
- User privilege escalation
- Man-in-the-middle attacks
- Viruses, Trojans and worms
- Zero-day vulnerabilities

IX. The Canaudit Security Script

- Understanding the script
- Running the script
- Analyzing the results
- Documenting the issues

X. The Canaudit Audit Security Checklists

- Consolidated Audit and Security Checklist