

**Enterprise Linux Security Administration**

**Course Number:** LNX-122  
**Duration:** 5 days

**Overview**

This Enterprise Linux Security Administration training course teaches attendees how to properly secure machines running the Linux operating system. Students gain an excellent understanding of potential security vulnerabilities and learn a broad range of general hardening techniques.

NOTE: This class can be taught using the Linux distribution of your choice.

**Prerequisites**

This class covers advanced security topics and is intended for experienced systems administrators. Candidates should have current Linux or UNIX systems administration experience equivalent to Accelebrate’s [Linux Fundamentals](file:////training/linux-fundamentals), [Enterprise Linux Systems Administration](file:////training/enterprise-linux-system-administration), and [Enterprise Linux Network Services](file:////training/enterprise-linux-network-services) courses.

**Materials**

All Linux training attendees receive comprehensive courseware.

**Software Needed on Each Student PC**

Attendees will not need to install any software on their computer for this class. The class will be conducted in a remote environment that Accelebrate will provide; students will only need a local computer with a web browser and a stable Internet connection. Any recent version of Microsoft Edge, Mozilla Firefox, or Google Chrome will be fine.

**Objectives**

* Gain an excellent understanding of potential security vulnerabilities
* Packet filtering, password policies, and file integrity checking
* How to audit existing machines and
* How to securely deploy new network services.
* How to use advanced security technologies such as Kerberos and SELinux

**Outline**

* introduction
* Security Concepts
  + Basic Security Principles
  + RHEL7 Default Install
  + RHEL7 Firewall
  + SLES12 Default Install
  + SUSE Basic Firewall Configuration
  + SLES12: File Security
  + Minimization – Discovery
  + Service Discovery
  + Hardening
  + Security Concepts
* Scanning, Probing, and Mapping Vulnerabilities
  + The Security Environment
  + Stealth Reconnaissance
  + The WHOIS database
  + Interrogating DNS
  + Discovering Hosts
  + Discovering Reachable Services
  + Reconnaissance with SNMP
  + Discovery of RPC Services
  + Enumerating NFS Shares
  + Nessus/OpenVAS Insecurity Scanner
  + Configuring OpenVAS
  + Intrusion Detection Systems
  + Snort Rules
  + Writing Snort Rules
* Password Security and PAM
  + Unix Passwords
  + Password Aging
  + Auditing Passwords
  + PAM Overview
  + PAM Module Types
  + PAM Order of Processing
  + PAM Control Statements
  + PAM Modules
  + pam\_unix
  + pam\_cracklib.so
  + pam\_pwcheck.so
  + pam\_env.so
  + pam\_xauth.so
  + pam\_tally2.so
  + pam\_wheel.so
  + pam\_limits.so
  + pam\_nologin.so
  + pam\_deny.so
  + pam\_warn.so
  + pam\_securetty.so
  + pam\_time.so
  + pam\_access.so
  + pam\_listfile.so
  + pam\_lastlog.so
  + pam\_console.so
* Secure Network Time Protocol (NTP)
  + The Importance of Time
  + Hardware and System Clock
  + Time Measurements
  + NTP Terms and Definitions
  + Synchronization Methods
  + NTP Evolution
  + Time Server Hierarchy
  + Operational Modes
  + NTP Clients
  + Configuring NTP Clients
  + Configuring NTP Servers
  + Securing NTP
  + NTP Packet Integrity
  + Useful NTP Commands
* Kerberos Concepts and Components
  + Common Security Problems
  + Account Proliferation
  + The Kerberos Solution
  + Kerberos History
  + Kerberos Implementations
  + Kerberos Concepts
  + Kerberos Principals
  + Kerberos Safeguards
  + Kerberos Components
  + Authentication Process
  + Identification Types
  + Logging In
  + Gaining Privileges
  + Using Privileges
  + Kerberos Components and the KDC
  + Kerberized Services Review
  + KDC Server Daemons
  + Configuration Files
  + Utilities Overview
* Implementing Kerberos
  + Plan Topology and Implementation
  + Kerberos 5 Client Software
  + Kerberos 5 Server Software
  + Synchronize Clocks
  + Create Master KDC
  + Configuring the Master KDC
  + KDC Logging
  + Kerberos Realm Defaults
  + Specifying [realms]
  + Specifying [domain\_realm]
  + Allow Administrative Access
  + Create KDC Databases
  + Create Administrators
  + Install Keys for Services
  + Start Services
  + Add Host Principals
  + Add Common Service Principals
  + Configure Slave KDCs
  + Create Principals for Slaves
  + Define Slaves as KDCs
  + Copy Configuration to Slaves
  + Install Principals on Slaves
  + Synchronization of Database
  + Propagate Data to Slaves
  + Create Stash on Slaves
  + Start Slave Daemons
  + Client Configuration
  + Install krb5.conf on Clients
  + Client PAM Configuration
  + Install Client Host Keys
* Administering and Using Kerberos
  + Administrative Tasks
  + Key Tables
  + Managing Keytabs
  + Managing Principals
  + Viewing Principals
  + Adding, Deleting, and Modifying Principals
  + Principal Policy
  + Overall Goals for Users
  + Signing Into Kerberos
  + Ticket types
  + Viewing Tickets
  + Removing Tickets
  + Passwords
  + Changing Passwords
  + Giving Others Access
  + Using Kerberized Services
  + Kerberized FTP
  + Enabling Kerberized Services
  + OpenSSH and Kerberos
* Securing the Filesystem
  + Filesystem Mount Options
  + NFS Properties
  + NFS Export Option
  + NFSv4 and GSSAPI Auth
  + Implementing NFSv4
  + Implementing Kerberos with NFS
  + GPG – GNU Privacy Guard
  + File Encryption with OpenSSL
  + File Encryption With encfs
  + Linux Unified Key Setup (LUKS)
* Aide
  + Host Intrusion Detection Systems
  + Using RPM as a HIDS
  + Introduction to AIDE
  + AIDE Installation
  + AIDE Policies
  + AIDE Usage
* Accountability with Kernel Auditd
  + Accountability and Auditing
  + Simple Session Auditing
  + Simple Process Accounting & Command History
  + Kernel-Level Auditing
  + Configuring the Audit Daemon
  + Controlling Kernel Audit System
  + Creating Audit Rules
  + Searching Audit Logs
  + Generating Audit Log Reports
  + Audit Log Analysis
* Selinux
  + DAC vs. MAC
  + Shortcomings of Traditional Unix Security
  + AppArmor
  + SELinux Goals
  + SELinux Evolution
  + SELinux Modes
  + Gathering SELinux Information
  + SELinux Virtual Filesystem
  + SELinux Contexts
  + Managing Contexts
  + The SELinux Policy
  + Choosing an SELinux Policy
  + Policy Layout
  + Tuning and Adapting Policy
  + Booleans
  + Permissive Domains
  + Managing File Context Database
  + Managing Port Contexts
  + SELinux Policy Tools
  + Examining Policy
  + SELinux Troubleshooting
  + SELinux Troubleshooting Continued
* Securing Apache
  + Apache Overview
  + httpd.conf – Server Settings
  + Configuring CGI
  + Turning Off Unneeded Modules
  + Delegating Administration
  + Apache Access Controls (mod\_access)
  + HTTP User Authentication
  + Standard Auth Modules
  + HTTP Digest Authentication
  + TLS Using mod\_ssl.so
  + Authentication via SQL
  + Authentication via LDAP
  + Authentication via Kerberos
  + Scrubbing HTTP Headers
  + Metering HTTP Bandwidth
* Securing PostgreSQL
  + PostgreSQL Overview
  + PostgreSQL Default Config
  + Configuring TLS
  + Client Authentication Basics
  + Advanced Authentication
  + Ident-based Authentication
* Securing Email Systems
  + SMTP Implementations
  + Security Considerations
  + chrooting Postfix
  + Email with GSSAPI/Kerberos Auth
* Conclusion