

Course Length: 5 days

Course Description: This highly technical course focuses on properly securing machines running the Linux operating systems. A broad range of general security techniques such as packet filtering, password policies, and file integrity checking are covered. Advanced security technologies such as Kerberos and SELinux are taught. Special attention is given to securing commonly deployed network services. At the end of the course, students have an excellent understanding of the potential security vulnerabilities -- know how to audit existing machines, and how to securely deploy new network services.

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 the GL-120 "Linux Fundamentals, GL-250 "Red Hat Linux Systems Administration" and GL-275 "Red Hat Linux Network Services"

Distributions: This courses is currently supported on the latest releases of Red Hat Enterprise Linux.

Security Foundations

- Security Principles
- Post-installation Hardening
- Service Discovery, Minimization
- Scanning and Mapping Vulnerabilities
- Probing with DNS, SNMP, RPC, and NFS
- Nessus Insecurity Scanner
- Password Security and PAM

Secure Authentication with Kerberos

- Secure Time Synchronization with NTP
- ACLs for Secure NTP
- Kerberos History, Implementations, and Concepts
- Kerberos Principals, Safeguards, and Components
- Authentication Process and Identification Types
- KDC Server Daemons
- Plan Topology and Implementation
- Create KDC Databases and Administrators
- Add Host Principals and Common Service Principals
- Configure Slave KDC
- Client PAM Configuration
- Managing Keytabs
- Principals and Managing Principals
- MIT vs. Heimdal Principal Policy
- Using Kerberized Services
- Enabling Kerberized Services
- OpenSSH and Kerberos

Securing the Filesystem

- Filesystem Mount Options
- NFS Properties and NFS Export Option
- NFSv4 and GSSAPI Auth

- Implementing NFSv4
- File Encryption with GPG and OpenSSL
- Encrypted Loopback FS
- Using RPM as an IDS
- TripWire History and Concepts
- TripWire Installation, Policies, and Configuration
- TripWire Commands and General Operation

Securing Common Services

- Secure CGI with Apache
- Turning off Unneeded Modules
- Configuration Delegation and Scope
- ACL by IP Address
- HTTP User Authentication
- Standard Auth Modules
- HTTP Digest Authentication
- Authentication via SQL, LDAP, and Kerberos
- Scrubbing HTTP Headers
- Metering HTTP Bandwidth
- PostgreSQL Overview and Default Configuration
- SSL for PostgreSQL
- Authentication Methods and Advanced Authentication
- Ident-based Authentication
- PostgreSQL Kerberos Authentication
- Integrating Apache, PHP, and PostgreSQL Securely
- SMTP Overview and Implementations
- Selecting an MTA
- Security Considerations
- Postfix Overview
- Chrooting Postfix
- Connections and Relays
- SMTP AUTH & StartTLS/SSL
- Secure Cyrus IMAP Config
- Using GSSAPI/Kerberos Authentication

SELinux

- DAC vs. MAC Security
- Shortcomings of Traditional UNIX Security
- SELinux Goals, Terms, and Architecture
- Activating and Interfacing with SELinux
- SELinux commands and Roles
- Understanding and Modifying Policy Source
- File Context Files (*.fc)
- Type Enforcement Files (*.te)
- Using Booleans
- Policy Analysis
- Policy Customization