

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.

### Course Objectives:

- Understand security techniques and principles
- Learn to secure filesystems and common services
- Detect system compromise
- Understand system vulnerabilities
- Generate detailed audit reports
- Learn Discretionary Access Control (DAC)
- Manage Port Contexts
- Activating and Deactivating Apache Modules
- Securing email systems

**Audience:** System and network administrators working with wide network security and authentication.

**Prerequisites:** Experienced systems administrators with current Linux or UNIX systems administration.

**Number of Days:** 5 days

<p><b>1 Security Concepts</b>          Basic Security Principles          RHEL6 Default Install          RHEL6 Firewall          SLES11 Default Install          SLES11 Firewall          SLES11: File Security          Minimization - Discovery          Service Discovery          Hardening          Security Concepts</p> <p><b>2 Scanning, Probing, and Mapping Vulnerabilities</b>          The Security Environment          Stealth Reconnaissance          The WHOIS database          Interrogating DNS          Discovering Hosts</p>	<p><b>3 Password Security and PAM</b>          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</p>
---	--

	pam_env.so		Kerberized Clients
	pam_xauth.so		KDC Server Daemons
	pam_tally2.so		Configuration Files
	pam_wheel.so		Utilities Overview
	pam_limits.so	6	<b>Implementing Kerberos</b>
	pam_nologin.so		Plan Topology and Implementation
	pam_deny.so		Kerberos 5 Client Software
	pam_warn.so		Kerberos 5 Server Software
	pam_securetty.so		Synchronize Clocks
	pam_time.so		Create Master KDC
	pam_access.so		Configuring the Master KDC
	pam_listfile.so		KDC Logging
	pam_lastlog.so		Kerberos Realm Defaults
	pam_console.so		Specifying [realms]
4	<b>Secure Network Time Protocol (NTP)</b>		Specifying [domain_realm]
	The Importance of Time		Allow Administrative Access
	Hardware and System Clock		Create KDC Databases
	Time Measurements		Create Administrators
	NTP Terms and Definitions		Install Keys for Services
	Synchronization Methods		Start Services
	NTP Evolution		Add Host Principals
	Time Server Hierarchy		Add Common Service Principals
	Operational Modes		Configure Slave KDCs
	NTP Clients		Create Principals for Slaves
	Configuring NTP Clients		Define Slaves as KDCs
	Configuring NTP Servers		Copy Configuration to Slaves
	Securing NTP		Install Principals on Slaves
	NTP Packet Integrity		Create Stash on Slaves
	Useful NTP Commands		Start Slave Daemons
5	<b>Kerberos Concepts and Components</b>		Client Configuration
	Common Security Problems		Install krb5.conf on Clients
	Account Proliferation		Client PAM Configuration
	The Kerberos Solution		Install Client Host Keys
	Kerberos History	7	<b>Administering and using Kerberos</b>
	Kerberos Implementations		Administrative Tasks
	Kerberos Concepts		Key Tables
	Kerberos Principals		Managing Keytabs
	Kerberos Safeguards		Managing Principals
	Kerberos Components		Viewing Principals
	Authentication Process		Adding, Deleting, and Modifying Principals
	Identification Types		Principal Policy
	Logging In		Overall Goals for Users
	Gaining Privileges		Signing In to Kerberos
	Using Privileges		Ticket types
	Kerberos Components and the KDC		Viewing Tickets
	Kerberized Services Review		

	Removing Tickets		Gathering Information
	Passwords		SELinux Virtual Filesystem
	Changing Passwords		SELinux Contexts
	Giving Others Access		Managing Contexts
	Using Kerberized Services		The SELinux Policy
	Kerberized FTP		Choosing an SELinux Policy
	Enabling Kerberized Services		Policy Layout
	OpenSSH and Kerberos		Tuning and Adapting Policy
<b>8</b>	<b>Securing the Filesystem</b>		Booleans
	Filesystem Mount Options		Permissive Domains
	NFS Properties		Managing File Contexts
	NFS Export Option		Managing Port Contexts
	NFSv4 and GSSAPI Auth		SELinux Policy Tools
	Implementing NFSv4		Examining Policy
	Implementing Kerberos with NFS		SELinux Troubleshooting
	GPG - GNU Privacy Guard	<b>12</b>	<b>Securing Apache</b>
	File Encryption with OpenSSL		Apache Overview
	File Encryption with encfs		httpd.conf - Server Settings
	Linux Unified Key Setup (LUKS)		Configuring CGI
<b>9</b>	<b>AIDE</b>		Turning Off Unneeded Modules
	Host Intrusion Detection Systems		Delegating Administration
	Using RPM as a HIDS		Apache Access Controls (mod_access)
	Introduction to AIDE		HTTP User Authentication
	AIDE Installation		Standard Auth Modules
	AIDE Policies		HTTP Digest Authentication
	AIDE Usage		Authentication via SQL
<b>10</b>	<b>Accountability with Kernel Audit</b>		Authentication via LDAP
	Accountability and Auditing		Authentication via Kerberos
	Simple Session Auditing		Scrubbing HTTP Headers
	Simple Process Accounting & Command		Metering HTTP Bandwidth
	History	<b>13</b>	<b>Securing PostgreSQL</b>
	Kernel-Level Auditing		PostgreSQL Overview
	Configuring the Audit Daemon		PostgreSQL Default Config
	Controlling Kernel Audit System		Configuring SSL
	Creating Audit Rules		Client Authentication Basics
	Searching Audit Logs		Advanced Authentication
	Generating Audit Log Reports		Ident-based Authentication
	Audit Log Analysis	<b>14</b>	<b>Appendix A – Securing Email Systems</b>
<b>11</b>	<b>SELinux</b>		SMTP Implementations
	DAC vs. MAC		Security Considerations
	Shortcomings of Traditional Unix		chrooting Postfix
	Security		Email with GSSAPI/Kerberos Auth
	AppArmor		
	SELinux Goals		
	SELinux Evolution		
	SELinux Modes		