

This five-day course helps the experienced Linux administrator develop advanced skills in configuring and managing a secure Linux network server. Students learn how to use the RPM system to create their own RPMs both for packaging your own software for standardized distribution, and for rebuilding existing packages from source RPMs. They will gain hands-on experience configuring and running essential network services, including DNS, NIS, DHCP, FTP, SSH, NTP, Samba, HTTP, Email, and LDAP. Finally, this course introduces important Linux security components, such as cryptography, Kerberos, SELinux, and network security.

Course Objectives:

- Provide instructions, within a spec file, for converting a source archive and patches into an RPM package.
- Configure the Kerberos network authentication protocol.
- Set up systems that synchronize their system clocks with the Network Time Protocol Server.
- Share files and printers with Windows systems using Samba.
- Configure the Apache HTTP server.
- Configure both a Sendmail and Postfix mail transfer agent.
- Use BIND to set up your system as a DNS server.
- Set up DHCP to deliver network information to client machines.
- Configure the VSFTP server to allow for file transfers using the FTP protocol.
- Use the cryptographic tool, openssl, to create keys, message digests, and digital certificates.
- Discuss different cryptography techniques and their application to systems used for securing data transfers.
- Use SSH as a secure alternative to telnet or rlogin.
- Secure services such as portmap, NFS, and DNS.
- Use NIS to provide centralized access to data.
- Set up an LDAP directory service.
- Configure Security Enhanced Linux (SELinux) as a second layer of protection that runs on top of traditional Discretionary Access Control.

Audience: Experienced Linux system administrators needing to set up or manage secure, enterprise-level network servers.

Prerequisites: *Linux Level 3* or equivalent experience.

Number of Days: 5 days

1	Rebuilding Packages The Red Hat Package Manager Why Create Your Own RPMs Building RPMs Packaging Open Source Software The Build Process Spec File	Spec File: Preamble (Header) Section Spec File: %Prep Section Spec File: %build Section Spec File: %install Section Spec File: %clean Section Spec File: Scriptlets Section
----------	--	--

- Spec File: %files Section
- Spec File: %changelog Section
- rpmbuild
- Signing RPM Packages - GnuPG
- Testing
- Custom RPM Guidelines
- 2. **Kerberos**
 - Kerberos Principles
 - Initial Kerberos Authentication
 - Ticket Authentication
 - Basic Realm Configuration
 - Installing a Master Key Distribution Center
 - DNS and Kerberos
 - kdc.conf
 - kadm5.acl
 - kadmin
 - Application Servers
 - Kerberos Clients
 - Troubleshooting Kerberized Services
 - Kerberos Security
 - Preauthentication
 - Ticket Validation
 - Trusting Other Realms
 - Kerberos Encryption
 - Kerberos Service Profile
- 3. **Network Time Protocol**
 - What is NTP?
 - NTP Design Structure
 - Configuring a NTP Client
 - Configuring a NTP Server
 - Using NTP in an Enclosed Network
 - Specifying Restrictions
- 4. **Samba**
 - Samba Configuration
 - Sharing Files and Directories with Samba
 - Sharing Printers with Samba
 - Verifying the Configuration File
 - Samba accounts
 - Starting Samba
 - Using the smbclient command
 - Mounting Samba Shares
- 5. **Apache**
 - What is Apache?
 - Configuring Apache
- The Main Tab
- The Virtual Hosts Tab
- Configuring Virtual Hosts
- Server Settings
- Performance Tuning
- Starting and Stopping the httpd Daemon
- Administering Squid
- 6. **Email Services**
 - Mail Configuration
 - Mail Protocols
 - IMAP/POP3 Configuration
 - Mail servers
 - Mail User Agent Configuration
 - Configuration of Sendmail
 - Configuration of PostFix
- 7. **DNS & BIND**
 - DNS Overview
 - Introduction to BIND
 - BIND's Primary Configuration File
 - Zone Files
 - Using rndc
 - Using the GUI-based Tool
- 8. **DHCP**
 - Introduction to DHCP
 - Setup the DHCP Server
 - Syntax of the /etc/dhcpd.conf File
 - Global Settings
 - Declaring a Subnet
 - Shared Networks
 - Using allow and deny
 - Address Pools
 - Additional Settings
 - The /var/lib/dhcp/dhcpd.leases File
 - Starting dhcpd
 - Setting up a DHCP Client
- 9. **FTP Services**
 - Setting up a VSFTP Server
 - Setting up Anonymous Upload
 - FTP Security
 - Limiting Access to the VSFTP Server
 - Modifying the Banner

- FTP Logging
- 10. Cryptography**
 - Symmetric Cryptography
 - Asymmetric Cryptography
 - Network Security
 - Cryptographic Tools
 - Using OpenSSL
 - Cryptographic Hashes
 - Using Asymmetric Encryption
 - Key Distribution
 - Digital Certificates
 - Transport Layer Security
 - TLS/SSL Handshake
 - Creating a RSA Private Key
 - Creating a Certificate Signing Request
 - Establishing a Certificate Authority
 - Managing Certificate Expiration
 - Managing a Certificate Revocation List
- 11. Secure Shell**
 - Remote Access Weaknesses
 - Overview of the Secure Shell
 - Configuring the Secure Shell
 - User or Group Level Access Control
 - Using StrictModes
 - Features and Functionality of SSH
 - Authentication Methods
 - Additional SSH Notes
 - Using the Secure Shell Client
 - Commands
- 12. Securing Services**
 - Sever vulnerabilities
 - Securing portmap
 - NFS Security
 - BIND security
 - X Window Server
 - The /etc/services file
 - Disabling unneeded services
 - Kernel network parameters
- 13. NIS**
 - What is NIS?
 - Configuring a NIS Server
 - Setting up a NIS Client
 - NIS Server Configuration
 - Configuring NIS Slave Servers
- 14. LDAP**
 - What is LDAP?
 - LDAP terms
 - LDAP structure
 - Setting up a LDAP server
 - Migration tools
 - Using the ldapsearch command
 - Additional LDAP tools
 - Additional LDAP configuration
- 15. SELinux**
 - What is SELinux?
 - Setting SELinux Functionality during Installation
 - Setting SELinux Functionality after Installation
 - The RHEL SELinux policy
- 16. Appendix A – Preparing for Certification Exams**
- 17. Appendix B – Preparing for RHCE and RHCT Exams**
- 18. Appendix C – Preparing for the LPI Exams**
- 19. Appendix D – Preparing for the Linux+ Exam**