

Course Description: This course teaches Linux and/or UNIX systems administrators how to build skills at configuring common network services and security administration using Red Hat Linux. This course is updated for building skills on Red Hat Enterprise Linux 4!

Who Should Attend: Linux or UNIX system administrators who already have some real world experience with Red Hat Linux systems administration and want a first course in networking services and security will benefit from this course.

Prerequisites: Students should have taken RH133 Red Hat Linux System Administration or have equivalent experience with Red Hat Linux. Students should also have LAN/WAN fundamentals or equivalent and Internetworking with TCP/IP or equivalent.

Benefits of Attendance: Upon completion of this course, students will be able to:

- Setup a Red Hat Linux server.
- Configure common network services and security at a basic level.

Course Outline:

Introduction To Network Services

Red Hat Linux Network Components
Connecting Networks
Service Management
chkconfig
xinetd Services
The xinetd Daemon
Fault Analysis

Organizing Networked Systems

DNS Basics
Internet DNS Hierarchy
Name Server Hierarchy
Client-side DNS
Server-side DNS
Berkeley Internet Name Domain (BIND)
Configuring BIND
Configuration File Basics
Address Match Lists and acl
RNDNC
Zone Files
Main Record Types
Delegating Subdomains
Caching-only Name Server
BIND Utilities
BIND Syntax Utilities
Configuring the DHCP server

Network File Sharing Services

Configuring NFS services
Configuring FTP services
Samba Services
Samba Daemons
Configuring Samba
Configuring File and Directory Sharing
Printing to the Samba Server
Authentication Methods
Samba Client Tools: smbclient and smbmount

Electronic Mail Services

sendmail Features
Security and "Anti-Spam" Features
An Email Review
Simple Operational Overview
Main Configuration Files
sendmail Configuration with the m4 Macro Language
sendmail Client Configuration
Blacklisting Recipients
Debugging sendmail
Postfix
Using Postfix
Additional postfix Configuration Files
procmail Local Delivery

The HTTP Service

Apache Features
Apache Configuration
Apache Server Configuration
Virtual Hosts

Apache Namespace Configuration
CGI
Apache Encrypted Web Server
Squid Web Proxy Cache

Security Concerns And Policy

Security Terms
Basic Network Security
Which Services Are Running?
Remote Service Detection
Definitions of Security
Security Policy
Backup Policies

Authentication Services

Authentication Basics
Service Profile: PAM
PAM Operation
Core PAM Modules
Authentication Modules
Password Security
Password Policy
Resource Limits
User Access Control
Single User Mode
Authentication Troubleshooting
NIS Overview
NIS Server Topology
Configuring an NIS Server
NIS Client Configuration
NIS Troubleshooting

System Monitoring

Introduction to System Monitoring
File System Analysis
Set User and Group ID Permissions
Typical Problematic Permissions
EXT2 Filesystem Attributes
Monitoring Data Integrity with tripwire
Configuring tripwire
System Log Files
syslogd and klogd configuration
Advanced syslogd configuration
Log File Analysis
Monitoring and Limiting Processes
Monitoring Processes with top
Monitoring Processes Graphically
System Activity Reporting
Process Accounting Tools

Securing Networks

Packet Filtering Capabilities
Netfilter Architecture
Netfilter Packet Flow
Chain Operations
Rule targets
Rule Matching
Network Address Translation(NAT)
Connection Tracking

Rule persistence
The "Bastion Host"

Securing Services

SystemV Startup Control
Securing the Service
tcp_wrappers Configuration
Daemon Specification
Client Specification
Advanced Syntax
xinetd-based security
xinetd Access Control
Host Patterns
Advanced Security Options

Securing Data

The Need For Encryption
Cryptographic Building Blocks
Random Numbers
One-Way Hashes
Symmetric Encryption
Asymmetric Encryption
Public Key Infrastructures
Digital Certificates
Generating Digital Certificates
OpenSSH Overview
The OpenSSH
OpenSSH Authentication
Protecting Your Keys
Applications: RPM