

This five-day course provides students with the knowledge to perform system administration tasks relating to kernel management and system security. These topics include the proc filesystem configuration, kernel rebuilds and backups as well as log file maintenance. The course moves into security issues including physical security of the host and console, user and system accounts, network and firewall security and software security. The course ends with intrusion detection techniques.

### Course Objectives:

- Configure kernel settings on the fly and make these changes permanent.
- Load and unload kernel modules.
- Choose appropriate kernel settings, configure and rebuild a kernel.
- Modify syslogd to log appropriate system events.
- Manage log rotation and file sizes.
- Utilize zip, gzip, and tar to create backups.
- Protect a host from unauthorized reboots and BIOS changes.
- Create secure user accounts and detect unauthorized user access to the system.
- Protect access to the root account and create alternate methods to perform root activities.
- Search for weaknesses in filesystem security using third party tools, and increase filesystem protection.
- Configure PAM for user and filesystem limits and logging.
- Add firewall protection to your system.

**Audience:** Linux system administrators who want to build competency with kernel builds and system security.

**Prerequisites:** *Linux Level 2* or equivalent experience.

**Number of Days:** 5 days

- |  |  |
|--|--|
| <p><b>1. The proc File System</b><br/>         What is the proc File System?<br/>         Viewing System Information<br/>         Viewing Process Information<br/>         Viewing and Changing Kernel Features<br/>         The sysctl Command<br/>         The /etc/sysctl.conf File</p> <p><b>2. Loadable Kernel Modules</b><br/>         What are Loadable Kernel Modules?<br/>         Loading LKMs<br/>         Displaying LKMs<br/>         Unloading LKMs<br/>         Loading Modules that have<br/>             Dependencies</p> <p><b>3. Rebuilding the Kernel</b><br/>         Kernel Source Files</p> | <p>Extract the Source Files<br/>         Apply the Patch Files<br/>         Initial Configuration Steps<br/>         Configure the 2.4 Kernel<br/>         Configure the 2.6 Kernel<br/>         Building the Kernel<br/>         Using the New Kernel<br/>         Building a Red Hat Enterprise<br/>             Linux Kernel<br/>         Kernel Parameters</p> <p><b>4. Log File Administration</b><br/>         System Log Daemons<br/>         The /etc/syslog.conf File<br/>         The /etc/sysconfig/syslog File<br/>         Default System Log Files</p> |
|--|--|

- Using logrotate to Maintain Log Files
- Using logwatch to Monitor Log Files
- Using redhat-logviewer to Monitor Log Files
- Generating Messages with logger
- 5. Backups**
  - Backing Up Data
  - Backup Media
  - Backup Methods
  - Device Files
  - Using the dump and restore Commands
  - Using the tar Commands
  - Using the gzip Command
  - Using the zip Command
  - Using the bzip2 Command
  - Using the cpio Command
  - Additional Utilities
- 6. Security Overview**
  - What is Security?
  - Balance
  - Staying Up to Date
  - Documentation
  - Thinking like the Enemy
  - What is a Security Policy?
  - Step 1 - Initially Secure the System
  - Step 2 - Maintain System Security
  - Step 3 - Recovery
- 7. Physical Security**
  - What is Physical Security?
  - Access Protection
  - Protecting BIOS
  - Protecting the Boot Loader
  - Disabling Reboots
  - Using vlock
  - Devices
  - Natural Disasters
  - Hardware Error
  - Theft
- 8. Securing User Accounts**
  - Account Names
  - Mail Aliases
  - The /etc/passwd, /etc/shadow, /etc/group and /etc/gshadow Files
  - Displaying User Information
  - Users and their Passwords
  - Users with no Passwords
- Forcing Users to Change their Password
- Preventing Users from Changing their Password
- Application Accounts
- Same UID, Multiple User Accounts
- Setting Accounts Defaults
- Process Accounting
- Tools
- 9. Securing System Accounts**
  - Securing the Root Account
  - Root Password and Name
  - The root's PATH Variable
  - Physically Protecting the root Account
  - Disallowing root Access
  - Limiting Access to root via su
  - Enabling Automatic Logouts
  - Granting root Access via the sudo Command
  - Securing System Accounts
- 10. Securing The Filesystem**
  - File Permissions and Ownership
  - Disk Space Usage
  - Securing crontab and at
  - File Attributes
  - File System mount Options
  - Tools
- 11. PAM**
  - What is PAM?
  - Syntax of PAM configuration files
  - PAM categories
  - PAM controls
  - PAM Modules
  - Using PAM to alter the password policy
  - Using PAM to provide resource limits
  - Using PAM to limit services
  - Using PAM to limit access time to services
  - Disabling console privileges
  - Other PAM features
- 12. TCP Wrappers**

The configuration files  
Syntax of /etc/hosts.allow and  
/etc/hosts.deny  
Using tcp\_wrappers banners  
Logging tcp\_wrappers connections  
Avoiding using two configuration files  
Using spawn and twist  
Additional tcp\_wrappers options

**13. Firewalls**

Kernel level firewalls in Linux  
Overview of iptables  
Overview of filtering packets  
Filtering incoming packets on the local  
system  
Filtering outgoing packets on the local  
system  
Using NAT  
Saving tables

**14. The xinetd Service**

The /etc/xinetd.conf File  
The /etc/xinetd.d Directory  
Important Attributes for xinetd-based  
Services  
Additional xinetd Considerations

**15. Intrusion Detection**

Performing the intrusion detection  
Monitoring network activity  
Probing for modified files  
Third party tools

**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**