Red Hat Server Hardening (RH413)

Modality: Virtual Classroom

Duration: 5 Days

About this Course:

Many companies endorse specific security policies and require a standard administration system to deal with user authentication problems, including:

- Application of updates
- System auditing and logging
- File system integrity

The RH413 course of Red Hat Server Hardening addresses all policy and configuration issues.

This course is the optimal guide to prepare fully for the Certification Examination of the Red Hat Certificate of Expertise in Server Hardening.

Course Objectives:

At the end of this course, students will be able to:

- Have a strong concept of Errata and its application within the Red Hat Enterprise Linux
- Use and apply special permission
- Use file system access control lists
- Manage user requirements
- Manage password aging policy
- Install, configure, and run Red Hat identity management tools
- Understand the concept of system auditing fully

Audience:

The following audience is suitable for this course:

- Technical people who want to understand the concept of Red Hat Enterprise Linux System
- IT officers who are responsible for the security and privacy for the Red Hat Enterprise Linux System, which yields consistent, reproducible, and scalable results
- Individuals who want to enhance their system’s security policy
- Individuals who are responsible for security requirements such as management and operating critical system and software updates
- RHCE-level skills

Prerequisites:

An ideal candidate must have Red Hat Certified Engineer (RHCE) certification, Red Hat Certified

Systems Administrator (RHCSA) certification, or skills and knowledge equivalent to it.

Candidates who do not fulfill this requirement can take these certification exams online.

Course Outline:

Track security updates
Understand how Red Hat Enterprise Linux produces updates and how to use yum to perform queries to identify what errata are available.
Manage software updates
Develop a process for applying updates to systems including verifying properties of the update.
Create file systems
Allocate an advanced file system layout and use file system encryption.
Manage file systems
Adjust file system properties through security related options and file system attributes.
Manage special permissions
Work with set user ID (SUID), set group ID (SGID), and sticky (SVTX) permissions and locate files with these permissions enabled.
Manage additional file access controls
Modify default permissions applied to files and directories; work with file access control lists.
Monitor for file system changes
Configure software to monitor the files on your machine for changes.
Manage user accounts
Set password-aging properties for users; audit user accounts.
Manage pluggable authentication modules (PAMs)
Apply changes to PAMs to enforce different types of rules on users.
Secure console access
Adjust properties for various console services to enable or disable settings based on security.
Install central authentication
Install and configure a Red Hat Identity Management server and client.
Manage central authentication
Configure Red Hat Identity Management rules to control both user access to client systems and additional privileges granted to users on those systems.
Configure system logging
Configure remote logging to use transport layer encryption and manage additional logs generated by remote systems.
Configure system auditing
Enable and configure system auditing.
Control access to network services
Manage firewall rules to limit connectivity to network services.