



RH413: Red Hat® Server Hardening

Outline for this course:

- 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.