Red Hat Security: Linux in Physical, Virtual and Cloud (RH415VT)

Modality: Virtual Classroom

Duration: 5 Days

About this course:

Manage security of Red Hat Enterprise Linux systems deployed in bare-metal, virtual, and cloud environments

Red Hat Security: Linux in Physical, Virtual, and Cloud (RH415) is designed for security administrators and system administrators who need to manage the secure operation of servers running Red Hat® Enterprise Linux®, whether deployed on physical hardware, as virtual machines, or as cloud instances.

This course is based on Red Hat Enterprise Linux 7.5, Red Hat Satellite 6.3, Red Hat Ansible® Engine 2.5, Red Hat Ansible Tower 3.2, and Red Hat Insights.

Maintaining security of computing systems is a process of managing risk through the implementation of processes and standards backed by technologies and tools. In this course, you will learn about resources that can be used to help you implement and comply with your security requirements.

Course Objective:

- Manage compliance with OpenSCAP.
- Enable SELinux on a server from a disabled state, perform basic analysis of the system policy, and mitigate risk with advanced SELinux techniques.
- Proactively identify and resolve issues with Red Hat Insights.
- Monitor activity and changes on a server with Linux Audit and AIDE.
- Protect data from compromise with USBGuard and storage encryption.
- Manage authentication controls with PAM.
- Manually apply provided Ansible Playbooks to automate mitigation of security and compliance issues.
- Scale OpenSCAP and Red Hat Insights management with Red Hat Satellite and Red Hat Ansible Tower.

Audience:

- System administrators, IT security administrators, IT security engineers, and other professionals responsible for designing, implementing, maintaining, and managing the security of Red Hat Enterprise Linux systems and ensuring their compliance with the organization's security policies.

Prerequisite:

- Be a Red Hat Certified Engineer (RHCE®), or demonstrate equivalent Red Hat Enterprise

Linux knowledge and experience

Course Outline:

Manage security and risk

Define strategies to manage security on Red Hat Enterprise Linux servers.

Automate configuration and remediation with Ansible

Remediate configuration and security issues with Ansible Playbooks.

Protect data with LUKS and NBDE

Encrypt data on storage devices with LUKS and use NBDE to manage automatic decryption when servers are booted.

Restrict USB device access

Protect system from rogue USB device access with USBGuard.

Control authentication with PAM

Manage authentication, authorization, session settings, and password controls by configuring pluggable authentication modules (PAMs).

Record system events with audit

Record and inspect system events relevant to security, using the Linux kernel's audit subsystem and supporting tools.

Monitor file system changes

Detect and analyze changes to a server's file systems and their contents using AIDE.

Mitigate risk with SELinux

Improve security and confinement between processes by using SELinux and advanced SELinux techniques and analyses.

Manage compliance with OpenSCAP

Evaluate and remediate a server's compliance with security policies by using OpenSCAP.

Automate compliance with Red Hat Satellite

Automate and scale your ability to perform OpenSCAP checks and remediate compliance issues using Red Hat Satellite.

Analyze and remediate issues with Red Hat Insights

Identify, detect, and correct common issues and security vulnerabilities with Red Hat Enterprise Linux systems by using Red Hat Insights.

Perform a comprehensive review

Review the content covered in this course by completing hands-on review exercises.