Red Hat Security: Linux in Physical, Virtual, and Cloud

Course Duration: 40 Hours **Course Code : RH415**

1. Course Overview

The **Red Hat Security: Linux in Physical, Virtual, and Cloud (RH415)** course provides system administrators and security professionals with the knowledge and skills to **secure Red Hat Enterprise Linux (RHEL) systems across physical, virtual, and cloud environments**.

Participants learn to **implement security policies, harden systems, manage user authentication, and protect services** while ensuring compliance with enterprise security standards. The course covers **firewalls, Selina, auditing, system hardening, and cloud security practices**, with hands-on labs in diverse environments.

2. What You'll Learn

- Implement **security policies and best practices** for RHEL systems.
- Configure **firewalls, Selina, and access controls**.
- Manage **users, groups, and authentication mechanisms** securely.
- Harden systems in **physical, virtual, and cloud environments**.
- Monitor and audit systems using **security and compliance tools**.
- Apply **secure service configurations and network protections**.
- Troubleshoot and mitigate security incidents.
- Ensure **enterprise-wide compliance and operational security**.

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

3. Target Audience

This course is intended for:

- Linux system administrators are responsible for **enterprise security**.
- Security engineers implement **system hardening and compliance**.
- Cloud and virtualization engineers managing **RHEL workloads securely**.
- DevOps and IT professionals focused on **multi-environment security management**.

4. Pre-Requisites

Participants should have:

- Red Hat Certified System Administrator (**RHCSA**) or equivalent experience.
- Basic understanding of **Linux system administration and networking**.
- Familiarity with **virtualization, cloud platforms, or container environments** is helpful.

5. Course Content

Module 1: Security Fundamentals in RHEL

- Security concepts and policies
- Threat modeling and risk assessment

Module 2: User and Authentication Management

- Managing users, groups, and permissions
- Configuring PAM and Kerberos authentication

Module 3: System Hardening

- Applying security baselines
- Kernel and system-level hardening

Module 4: Selina Administration

- Selina modes, policies, and troubleshooting
- Implementing mandatory access controls

Module 5: Firewall and Network Security

- Configuring **firewall** and network zones
- Securing network services and ports

Module 6: Auditing and Logging

- Setting up system audit frameworks
- Monitoring and reviewing logs for compliance

Module 7: Cloud and Virtualization Security

- Securing virtual machines and cloud instances
- Best practices for hybrid deployments

Module 8: Service and Application Security

- Securing web, database, and email services
- Implementing TLS/SSL and certificates

Module 9: Troubleshooting and Incident Response

- Diagnosing security issues
- Recovering compromised systems

Module 10: Hands-On Labs

- Real-world security scenarios
- Implementing hardening and auditing across environments