Red Hat Security: Identity Management and Authentication

Course Duration: 40 Hours **Course Code RH362**

1. Course Overview

The **Red Hat Security: Identity Management and Authentication (RH362)** course equips system administrators and security professionals with the skills to deploy and manage **centralized identity, authentication, and access control** using **Red Hat Identity Management (IdM)**.

Participants learn to configure **Kerberos, LDAP, DNS, TLS certificates, host-based access control (HBAC)**, and establish **trust relationships with Active Directory (AD)**. The course also emphasizes **automation of IdM tasks using Ansible** to ensure secure, scalable, and efficient enterprise environments.

2. What You'll Learn

- Deploy and configure **IdM servers, clients, and replicas**.
- Manage **users, groups, roles, sudo rules, and HBAC policies** centrally.
- Implement **Kerberos-based authentication** across Linux systems.
- Use IdM as a **DNS server and Certificate Authority (CA)**.
- Establish and manage **trust relationships with Active Directory (AD)**.
- Automate IdM administration with **Ansible system roles**.

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

- Troubleshoot and secure **identity management and authentication services**.

3. Target Audience

This course is designed for:

- Linux system administrators responsible for **enterprise authentication and security**.
- Security engineers managing **access control and identity services**.
- IT architects and DevOps professionals integrating Linux systems with **Active Directory**.
- Professionals looking to enhance their skills in **centralized identity and authentication management**.

4. Pre-Requisites

Participants should have:

- Red Hat Certified System Administrator (**RHCSA**) or equivalent Linux administration knowledge.
- Familiarity with Linux command-line operations and basic system administration.
- Understanding of networking, authentication concepts (LDAP/Kerberos), and DNS is helpful.

5. Course Content

Module 1: Introduction to Identity Management (dims)

- Concepts, architecture, and benefits of dims

Module 2: Installing and Configuring Dime

- Setting up Dime servers, clients, and replicas
- Ensuring redundancy and scalability

Module 3: Centralized User and Group Management

- Managing users, groups, roles, and Sudo policies
- Role-based delegation

Module 4: Kerberos Authentication

- Understanding Kerberos workflows
- Configuring Kerberos-based authentication

Module 5: DNS and Service Discovery

- Configuring Dime as a DNS server
- Managing service records and domain integration

Module 6: Certificates and Public Key Infrastructure (PKI)

- Using ID's Certificate Authority (CA)
- Automating certificate requests, deployment, and renewal

Module 7: Active Directory Integration

- Cross-forest trust configuration
- Managing authentication in hybrid environments

Module 8: Host-Based Access Control (HBAC)

- Defining and enforcing HBAC policies
- Role-based access control and security delegation

Module 9: Automation with Ansible

- Using Ansible system roles for Dime management
- Automating repetitive identity management tasks

Module 10: Security, Hardening, and Troubleshooting

- Enhancing Dime security
- Troubleshooting Dime replication, authentication, and service issues

Module 11: Hands-On Labs

- End-to-end practice with Dime configuration, Active Directory integration, HBAC policies, and automation

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