

## Course Overview

RHS429 introduces advanced system administrators, security administrators, and applications programmers to SELinux policy writing. Participants in this course will learn how SELinux works; how to manage SELinux; and how to write an SELinux policy. This class culminates in a major project to scope out and then write policies for previously unprotected services

## Prerequisites:

RHS429 requires RHCE-level skills. Prerequisite skills can be shown by passing the RHCE Exam or by taking RH253/RH254 or by possessing comparable skills and knowledge.

## Target Audience

RHS429 is designed for computer security specialists and administrators responsible for setting & implementing security policies on a Linux computer. Applications programmers also may consider taking the course to understand how to provide a set of SELinux policies for third party applications.

## Course Outline

### Unit 1 - Introduction to SELinux

- Discretionary Access Control vs. Mandatory Access Control
- SELinux History and Architecture Overview
- Elements of the SELinux security model: ?user identity and role
  - domain and type
  - sensitivity and categories
  - security context
- SELinux Policy and Red Hat's Targeted Policy
- Configuring Policy with Booleans
- Archiving
- Setting and Displaying Extended Attributes
- Hands-on Lab: Understanding SELinux

### Unit 2 - Using SELinux

- Controlling SELinux
- File Contexts
- Relabeling Files and Filesystems
- Mount options
- Hand-on Lab: Working with SELinux

### Unit 3 - The Red Hat Targeted Policy

- Identifying and Toggling Protected Services
- Apache Security Contexts and Configuration Booleans
- Name Service Contexts and Configuration Booleans
- NIS Client Contexts
- Other Services
- File Context for Special Directory Trees
- Troubleshooting and avc Denial Messages
- setroubleshoot and Logging
- Hands-on Lab: Understanding and Troubleshooting the Red Hat Targeted Policy

### Unit 4 - Introduction to Policies

- Policy Overview and Organization
- Compiling and Loading the Monolithic Policy and Policy Modules
- Policy Type Enforcement Module Syntax
- Object Classes
- Domain Transition
- Hands-on Lab: Understanding policies

### Unit 5 - Policy Utilities

- Tools available for manipulating and analyzing policies ?apol
  - seaudit and seaudit\_report
  - checkpolicy
  - sepcut
  - serearch
  - sestatus
  - audit2allow and audit2why

- sealert
- avcstat
- seinfo
- semanage and semodule
- Man pages
- Hands-on Lab: Exploring Utilities

### Unit 6 - User and Role Security

- Role-based Access Control
- Multi Category Security
- Defining a Security Administrator
- Multi-Level Security
- The strict Policy
- User Identification and Declaration
- Role Identification and Declaration
- Roles in Use in Transitions
- Role Dominance
- Hands-on Lab: Implementing User and Role Based Policy Restrictions

### Unit 7 - Anatomy of a Policy

- Policy Macros
- Type Attributes and Aliases
- Type Transitions
- When and How do Files Get Labeled
- restorecond
- Customizable Types
- Hands-on Lab: Building Policies

### Unit 8 - Manipulating Policies

- Installing and Compiling Policies
- The Policy Language
- Access Vector
- SELinux logs
- Security Identifiers - SIDs
- Filesystem Labeling Behavior
- Context on Network Objects
- Creating and Using New Booleans
- Manipulating Policy by Example
- Macros
- Enableaudit
- Hands-on Lab: Compiling Policies

### Unit 9 - Project

- Best practices
- Create File Contexts, Types and Typealiases
- Edit and Create Network Contexts
- Edit and Create Domains
- Hands-on Lab: Editing and Writing Policy

**Course Duration:** Four Days: 10 am - 5.30 pm

**Course Fee Rs. 9,600/-**

(Plus Service Tax as applicable)