

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

Who Should Attend: RHS429 is designed for computer security specialists and other system administrators responsible for setting and implementing security policies on a Linux computer. Applications programmers also may consider taking the course to understand how to provide a set of SE Linux policies for third party applications. Participants need not have in depth knowledge of SE Linux, but should have a basic understanding of the SE Linux security layer. For example, SE Linux information as taught in RH133 or RH300 is sufficient.

Prerequisites: RHS429 requires RHCE-level skills. Prerequisite skills can be shown by passing the RHCE Exam in either RH302 or RH300, or by taking RH253 or by possessing comparable skills and knowledge.

Benefits of Attendance: Upon completion of this course, students will be able to:

- Understand how SE Linux operates within the Red Hat targeted policy.
- Understand how policies are written, compiled, and debugged.
- Create a set of policies from scratch for a previously unprotected service.
- Analyze the service, determining its security needs.
- Design and implement a set of policies.
- Test and fix the policies.
- Document the service's new policies so that others can effectively administer the service.

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:
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
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