Fundamentals of SELinux – Detailed Syllabus

Course Description
Our two-day, hands-on training courses will teach you how SELinux can bolster the security of your data, your systems, and your organization. Topics include:

- An overview of its access control architecture
- The specific security challenges it was developed to address
- The differences between SELinux and other access control or security mechanisms
- An understanding of Type Enforcement concepts
- The fundamentals of SELinux policy language and how to write and analyze an SELinux policy

2 Day Course Content:

- Introduction to SELinux
  - Benefits
  - References

- Access Control Overview
  - Access Control Concepts
  - Standard Linux access control
  - SELinux access control
  - Access control policies (DAC, MAC)
  - Linux and SELinux comparison

- SELinux Policy High Level Concepts
  - Policy enforcement decisions
  - SELinux modes
  - Security attributes and contexts
  - Type Enforcement Access Control
    - Types
    - Classes
    - Permissions
  - Privilege Levels
  - Benefits and Challenges of Type Enforcement

- Solving Security Challenges using SELinux
  - System Integrity
  - Application Integrity
  - Least Privilege
  - Controlled Information Flow
  - Assured Pipelines
  - Domain Isolation
  - System Hardening

- Implementation Strategies
Security Planning
Choosing an SELinux platform
Security Evaluation and Accreditation
SELinux Policy Configuration and Development
SELinux Policy Analysis
Maintenance Planning

SELinux Policy Language
- Types and Attributes
- Access Vector Rules
- Type Transition Rules
- Conditional Policy
- Roles
- Users
- Multi-Level Security
- Network Access Control

SELinux Policy Development
- Policy Development Steps
  - Workflow
  - Reading Audit Messages

Writing Reference Policy Modules
- Module-related constructs
- Encapsulation
- Interfaces and Abstraction
- Writing Interfaces
- Labeling policy

Write an SELinux policy (for an application) (hands-on exercise)
Perform analysis of an SELinux policy (hands-on exercise)