15.8 Security-Enhanced Linux (SELinux)

As you study this section, answer the following questions:

- How is SELinux a mandatory access control solution?
- What type of access controls can be enforced using SELinux?
- What is a SELinux policy? How is it used?
- What type of policies are used with SELinux?
- What are the two SELinux modes? How are they used?

Key terms for this section include the following:

Term	Definition
Security-Enhanced Linux (SELinux)	A Linux kernel security module that provides a strong and flexible mandatory access control (MAC) system for the Linux kernel. It can be used to enforce access control on resources based on variables, such as users and applications.
SELinux policy	SELinux policies are used to determine which items are protected and how. Policies are a set of rules that guide the SELinux security engine. Two types of policies exist, targeted and multi-level security (MLS).

This section helps you prepare for the following certification exam objectives:

Exam	Objective

CompTIA Linux+	3.1 Given a scenario, apply or acquire the appropriate user and/or group permissions and ownership.
	• Context-based permissions
	  ◦ SELinux configurations
	  ▪ disabled
	  ▪ permissive
	  ▪ enforcing
	  ◦ SELinux policy
	  ▪ targeted
	  ◦ SELinux tools
	  ▪ setenforce
	  ▪ getenforce
	  ▪ sestatus
	  ▪ setsebool
	  ▪ getsebool
	  ▪ chcon
	  ▪ restorecon
	  ▪ ls -Z
	  ▪ ps -Z
	4.3 Given a scenario, analyze and troubleshoot user issues.

	• Insufficient privileges for authorization ◦ SELinux violations 4.4 Given a scenario, analyze and troubleshoot application and hardware issues. • SELinux context violations