15.9 Application Armor (AppArmor)

As you study this section, answer the following questions:

- How does AppArmor help protect a Linux computer?
- How can you troubleshoot an application being protected by AppArmor?
- Using AppArmor, how can you determine which network sockets are vulnerable?
- What are the two major modes in which AppArmor profiles are run?
- What commands are used to change the mode an AppArmor profile uses?

Key terms for this section include the following:

Term	Definition
Mandatory Access Control (MAC)	A type of access control where the system (not a user) restricts individual resource owners' ability to grant or deny access to resource objects in a file system.
Complain	A processing mode in which the setting specified in an AppArmor not enforced, but violations are logged.
Enforce	A processing mode in which the setting specified in an AppArmor profile prevent applications from taking any restricted actions.

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 ◦ AppArmor ▪ aa-disable ▪ aa-complain ▪ aa-unconfined ▪ /etc/apparmor.d/ ▪ /etc/apparmor.d/tunables