15.2 User Security and Restriction

As you study this section, answer the following questions:

- What are the characteristics of a secure password?
- Which **chage** option sets the minimum number of days a user must keep a password?
- What type of resources are affected by the **ulimit** utility?
- When would you need to configure the /etc/security/limits.conf file?
- What is the syntax of the /etc/security/limits.conf file?
- What does file auditing allow you to do?

Key terms for this section include the following:

Term	Definition
Linux Pluggable Authentication Module (PAM)	PAM provides dynamic authentication support for applications and services in a Linux system, such as login and su.
Lightweight Directory Access Protocol (LDAP)	An open, vendor-neutral, industry-standard application protocol used to locate organizations, individuals, and other resources, such as files and devices in a network, on the internet or on a corporate intranet.
Teletypewriter (TTY)	Over the years, TTY has had many meanings. Early user terminals, which were connected to computers, were electromechanical teleprinters or teletypewriters (TeleTYpewriter, TTY). Since then, TTY has been used as the name for the text-only console; but now, this text-only console is a virtual console, not a physical console. On a Linux system, a new text-only console can be accessed (logged into) by pressing a combination of keys, such as Ctrl+Alt+F2 for TTY2.

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

Exam	Objective
TestOut Linux Pro	4.1 Manage users and groups. • Create and manage user accounts • Manage user access

CompTIA Linux+	2.2 Given a scenario, manage users and groups.
	• Modification
	  ◦ passwd
	• Queries
	  ◦ who
	  ◦ last

2.3 Given a scenario, create, modify, and redirect files.

- File and directory operations
    - find

2.6 Given a scenario, automate and schedule jobs.

- crontab

3.1 Given a scenario, apply or acquire the appropriate user and/or group permissions and ownership.

- File and directory permissions
    - Utilities
        - ulimit
        - chage

3.2 Given a scenario, configure and implement appropriate access and authentication methods.

- PAM
    - Password Policies
    - LDAP Integration
    - Required, allowed, or sufficient
    - /etc/pam.d/
    - pam_tally2
    - faillock
- TTYs
    - /etc/securetty
    - /dev/tty#
- PTYs

3.3 Summarize security best practices in a Linux environment.

- Importance of disabling or uninstalling unused and unsecure services
    - Finger