7.1.4 User and Group Facts

This lesson covers the following topics:

- User groups and types
- User and group databases
- Commands for managing password file entries

User Groups and Types

User accounts control the ability to log on to a system, access resources, and perform certain actions. Groups provide a way to group users for administrative purposes, such as assigning permissions to files.

Be aware of the following types of users and groups:

Type	Description
Standard user	Standard user accounts can log into the system. Standard user accounts: ▪ Have friendly usernames (such as Mary or bkaun). An administrator must create the usernames. ▪ Have an ID of 500 or more (on some distributions) or 1000 or more (on other distributions). The ID is automatically assigned by the system when the account is created.
System or service accounts	System user accounts (also called service user accounts) are created by default during the Linux installation and are used by the system for specific roles. System user accounts: ▪ Have names that correspond with their roles, such as ftp and mail. ▪ Cannot be used to log into the system. ▪ Have an ID of 500 or less (on some distributions) or 1000 or less (on other distributions). The ID is automatically assigned by the system when the account is created. The root user account is created by default and has a UID of 0; however, it can be used to log into a system and perform tasks.
Primary group	Primary groups (also called the private group) are created by default on most Linux distributions when a standard user is created and are used to manage access to files and directories. Primary groups: ▪ Have the corresponding user as the only member. ▪ Are automatically assigned as the owner of files and directories when they are created in the file system. ▪ Are similar to any other group. The only difference is that the group is identified as the primary group in the user account's configuration.
Secondary group	Secondary groups are also used to manage access to files and directories. Secondary groups: ▪ Are not automatically assigned user accounts as members. ▪ Receive their membership as assigned by the system administrator.

The following table explains the files where user and group databases are stored.

File	Description
/etc/passwd	The /etc/passwd file holds user account information. Be aware of the following details: ▪ Each entry identifies a user account. ▪ Each entry contains multiple fields, with each field separated by a colon. The following line is a sample entry in the /etc/passwd file: pclark:x:501:501:Petunia Clark:/home/pclark:/bin/bash The fields within this line are as follows: ▪ User account name. ▪ Password. An x in the field indicates passwords are stored in the /etc/shadow file. ▪ User ID number.

	▪ Primary group ID number (also known as the GID). ▪ Description field. This field is typically used for the user's full name. ▪ Path to the home directory. ▪ Path to the default shell.

/etc/shadow	The /etc/shadow file holds passwords and password expiration information for user accounts. Be aware of the following details:
	▪ Using the /etc/shadow file to separate usernames from passwords increases the security of the user passwords.
	▪ Like the /etc/passwd file, each entry corresponds to a user account and each entry contains multiple fields, with each field separated by a colon.
	The following line is a sample entry in the /etc/shadow file:
	pclark:$ab7Y56gu9bs:12567:0:99999:7:::
	The fields within this line are as follows:
	▪ User account name.
	▪ Password.
	  ▪ $ preceding the password identifies the password as an encrypted entry.
	  ▪ ! or !! indicates that the account is locked and cannot be used to log in.
	  ▪ * indicates a system account entry and cannot be used to log in.
	▪ Last change. The date of the most recent password change measured in the number of days since 1 January 1970.
	▪ Minimum password age. The minimum number of days the user must wait before changing the password.
	▪ Maximum password age. The maximum number of days between password changes.
	▪ Password change warning. The number of days a user is warned before the password must be changed.
	▪ Grace logins. The number of days the user can log in without changing the password.
	▪ Disable time. The number of days since 1 January 1970, after which the account will be disabled.

/etc/group	The /etc/group file holds group information including the group name, GID, and group membership information. Be aware of the following details: ▪ Each entry identifies a group. ▪ Each entry contains multiple fields, with each field separated by a colon. The following line is a sample entry in the /etc/group file: sales:x:510:pclark,mmckay,hsamson The fields within this line are as follows: ▪ Group name. ▪ Group password. An x indicates the group passwords are contained in the /etc/gshadow file. ▪ Group ID. ▪ Group members (contains a comma-separated list of user accounts that are members of the group).

/etc/gshadow	The /etc/gshadow file holds passwords for groups. Be aware of the following details:
	▪ Like the /etc/group file, each line corresponds to a group.
	▪ Each line consists of fields separated by colons.
	The following line is a sample entry in the /etc/gshadow file:
	sales:!:pclark:pclark,mmckay,hsamson
	The fields within this line are as follows:
	▪ Group name.
	▪ Group password. The group password allows users to add themselves as members of the account.
	  ▪ If the field contains a single exclamation point (!), the group account cannot be accessed using the password.
	  ▪ If the field contains a double exclamation point (!!), no password has been assigned to the group account (and it cannot be accessed using the password).
	  ▪ If there is no value, only group members can log in to the group account.
	▪ Administrators. Contains a comma-separated list of users who have authorization to administer the account.
	▪ Group members. Contains a comma-separated list of user accounts that are members of the group.

Commands for Managing Password File Entries

Additional commands for managing file entries include the following:

Command	Description
pwck	Verifies the entries in the /etc/passwd and /etc/shadow files to ensure that they have the proper format and contain valid data. Errors are displayed on the screen, and entries may be deleted to solve the errors. For example, checks are made to verify that each entry has: ▪ The correct number of fields ▪ A unique and valid user name ▪ A valid user and group identifier ▪ A valid primary group ▪ A valid home directory ▪ A valid login shell
pwconv	The **pwconv** command is used to move passwords from the less-secure /etc/passwd file to the more secure /etc/shadow file. The opposite of this action can be done with the **pwunconv** command and will also remove the shadow file. Today, however, virtually all Linux distributions ship with shadow files enabled by default. The synchronization process is as follows: ▪ The entries in the shadowed file that do not exist in the passwd file are removed. ▪ The shadowed entries that don't have x as the password in the passwd file are updated. ▪ Any missing shadowed entries are added. ▪ Passwords found in the passwd file are replaced with x.