Operating Systems

Lecture 05: Managing User and Group Accounts

Managing User and Group Accounts

One of the benefits of Linux is

- Its multiuser capabilities. By creating and modifying user and group accounts, you can further tailor the Linux environment to the needs of your organization.
- You will also be able to provide individualized services to users after creating an account for them.

Managing User and Group Accounts

User Accounts

- A user account is a collection of information that defines a user on a system.
- It is the representation of a user on a computer.
- User account information includes the user name and password for the user to log in to the system, groups to which the user belongs, and rights and permissions that the user has to access the system and its resources.
- When an account is created, it is assigned a unique number that is called User ID (UID).

Managing User and Group Accounts

User Accounts

- **The useradd Command**
  - The syntax of the useradd command is useradd [options] {username}
  - You can use the **adduser** command to perform the same functions as the **useradd** command
  - Special user accounts are required to run processes associated with certain services. For example, daemon is a user account that is used to run the daemon service.
    - In special user accounts, the UID value for the users will be less than the default UID value, which is 500. Such special users will not have a home directory. You can create a special user account using the **useradd -r {special user name} command**.

Managing User and Group Accounts

User Accounts

- **The useradd Command**
  - Linux allows you to add user accounts by directly editing the password file. However, this is not recommended because you may damage your system if you accidentally leave something out or alter existing user accounts. If the system is damaged, nobody will be able to log in—not even the root user. In such a case, you will have to reinstall your system and redefine the user accounts.

Managing User and Group Accounts

User Accounts

- **The useradd Command**
  - Default User Accounts
    - Numerous user accounts are created by default upon system installation. Some of the main
    - user accounts are:
    - root
    - bin
    - daemon
    - ftp
    - sshd
    - nfsnobody
    - apache
    - And, squid

Managing User and Group Accounts

User Accounts

- **The useradd Command**
  - **The Role of the Root**
    - Every Linux system has at least one system administrator whose job is to maintain the system and make it available to users. This user is the root.
    - The root user can perform any task on the Linux system without restrictions.
    - System administrators are also responsible for adding new users to the system and for setting up their initial environment.
  - **Other Types of User Accounts**
    - **Local:** Local user accounts allow users to log in to single, specific computer systems.
    - **Domain:** Domain user accounts allow users to log in to a computer system. However, the identity of a user is recognized by all computers in the domain.
    - **Guest:** Guest accounts are built-in user accounts created at the time of installation.They are also known as anonymous accounts. Using an anonymous account, multiple users can log in to the system at the same time. Usually, anonymousaccounts do not require passwords.

Managing User and Group Accounts

User Accounts

- **Passwords**
  - Generally, when user accounts are created without passwords, they can be easily misused.
  - For this reason, when you create a user account, you should immediately set a password for the user using the passwd command.
  - In Linux, if a password is not set for the user account, the account gets locked automatically. This is to help prevent unauthorized access to the system.
  - You can change the password of your user account using the **passwd** command.
  - You cannot change the password for any other user account because the password command does not allow you to specify any other username.
  - Only the root user can change the password for other users by specifying the user name with the passwd command.

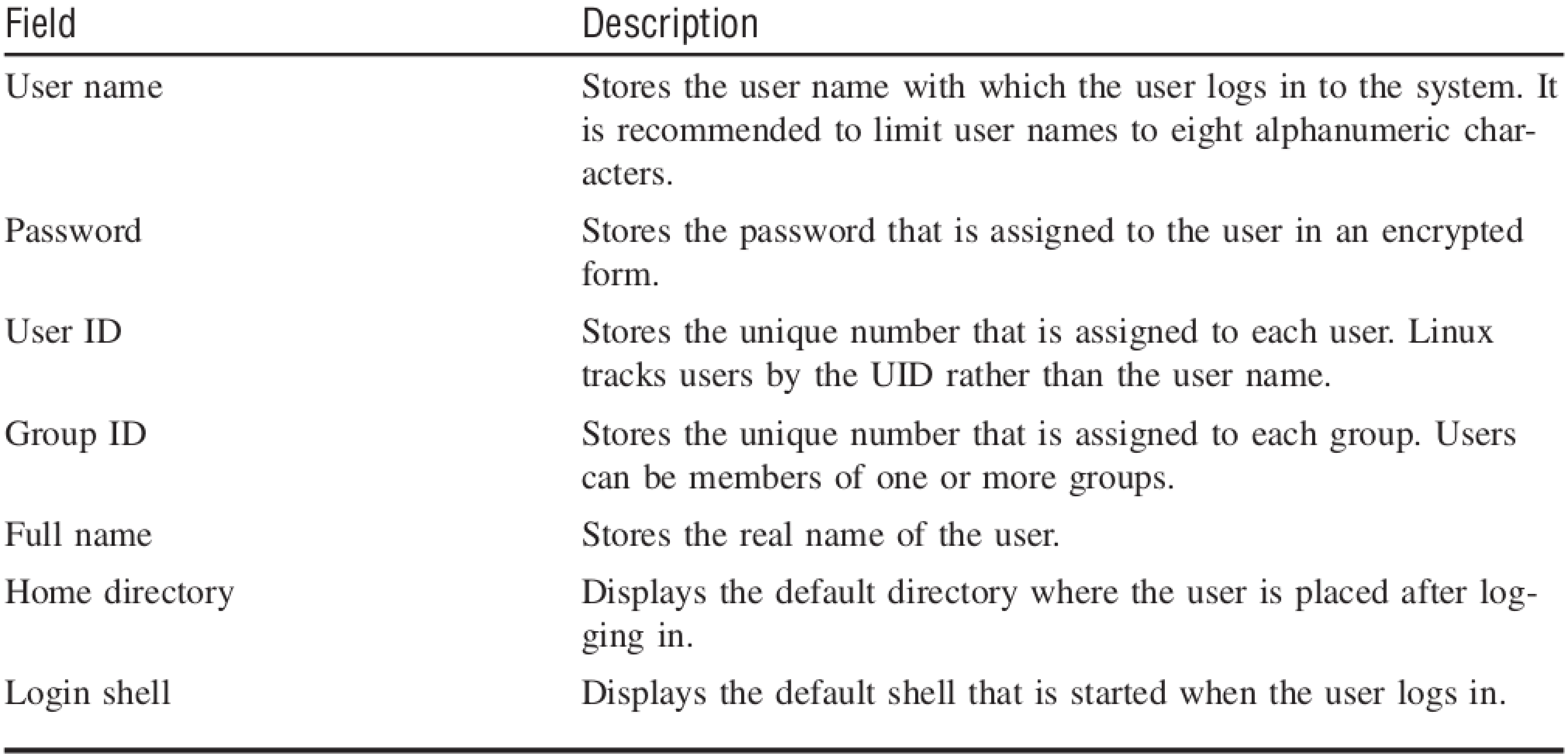
Managing User and Group Accounts

User Accounts

- **Passwords**
  - A root user can create a password for a user by entering *passwd [user name],* where [user name] is the name of the user for whom the password is set.
  - The password should contains capital, small letters, numbers, signs, and it should be more than 20 char length.
  - **The /etc/passwd File**
    - When you add a new user, information about the user is saved in the /etc/passwd file

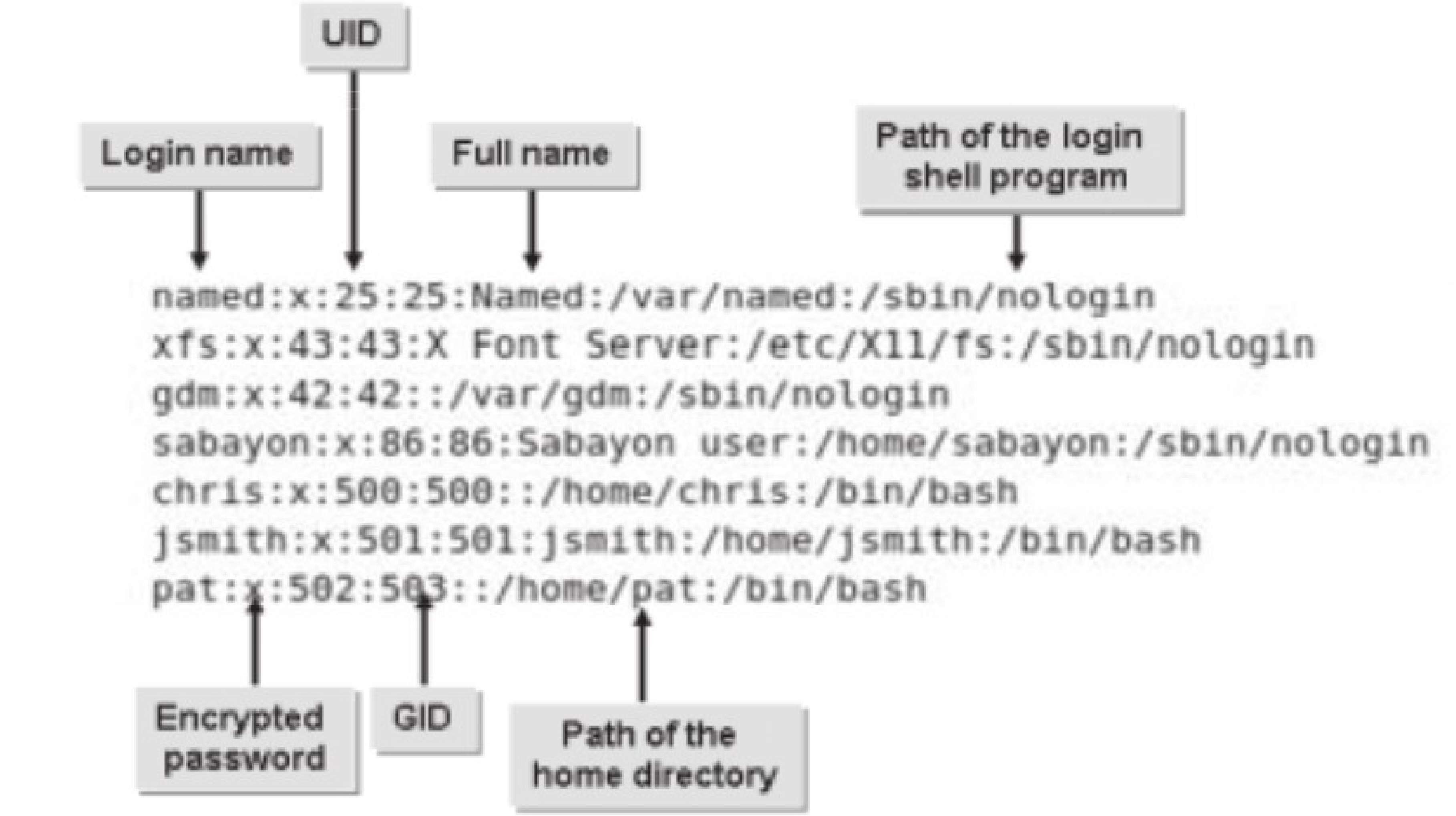
Managing User and Group Accounts

Fields in the *\/etc/passwd* file:



Field	Description
User name	Stores the user name with which the user logs in to the system. It is recommended to limit user names to eight alphanumeric characters.
Password	Stores the password that is assigned to the user in an encrypted form.
User ID	Stores the unique number that is assigned to each user. Linux tracks users by the UID rather than the user name.
Group ID	Stores the unique number that is assigned to each group. Users can be members of one or more groups.
Full name	Stores the real name of the user.
Home directory	Displays the default directory where the user is placed after logging in.
Login shell	Displays the default shell that is started when the user logs in.

Managing User and Group Accounts



```
named:x:25:25:Named:/var/named:/sbin/nologin
xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin
gdm:x:42:42::/var/gdm:/sbin/nologin
sabayon:x:86:86:Sabayon user:/home/sabayon:/sbin/nologin
chris:x:500:500::/home/chris:/bin/bash
jsmith:x:501:501:jsmith:/home/jsmith:/bin/bash
pat:x:502:503::/home/pat:/bin/bash
```

Managing User and Group Accounts

User Accounts

- **Shadow Passwords**
  - Each user's password is stored and encrypted in the /etc/passwd file.
  - This file needs to be readable, which makes copies of users' encrypted passwords easily obtainable to any person trying to attack the system. Then, by using various techniques, the attackers can decipher passwords.
  - You can overcome this problem by using shadow passwords. Shadow passwords store the encrypted passwords in a separate highly protected file, the /etc/shadow file. This file is readable only to the root user.
  - Therefore, it is less of a security risk compared to the /etc/passwd file because it becomes difficult for attackers to access the file, obtain the user passwords, and then decipher them. The /etc/passwd file also contains the account or password expiration values.

Managing User and Group Accounts

User Accounts

- **Shadow Passwords**
  - The /etc/shadow file contains the following information:
    - username: The user name.
    - passwd: The encoded password.
    - last: Number of days since the password was last changed.
    - may: Number of days before which the password may be changed.
    - must: Number of days after which the password must be changed.
    - warn: Number of days pending before which the password will expire.
    - expire: Number of days after which the password will expire and the user account will be disabled.
    - disable: Number of days since Jan 1, 1970, that the user account has been disabled.
    - reserved: A reserved field.

Managing User and Group Accounts

User Accounts

- **The id Command**
  - The id command is used to display UID and group ID (GID) information. Entering the command with no options displays information about the user who is currently logged in. You can also specify a user name as an option to display ID information about a specific user.
- **The finger Command**
  - The finger command is used to display information about users, including login name, real name, terminal name, write status, idle time, login time, office location, and office phone number. Some of these fields may be empty if no information was included when the user account was created. You can also view information about a specific user by entering finger [user name].

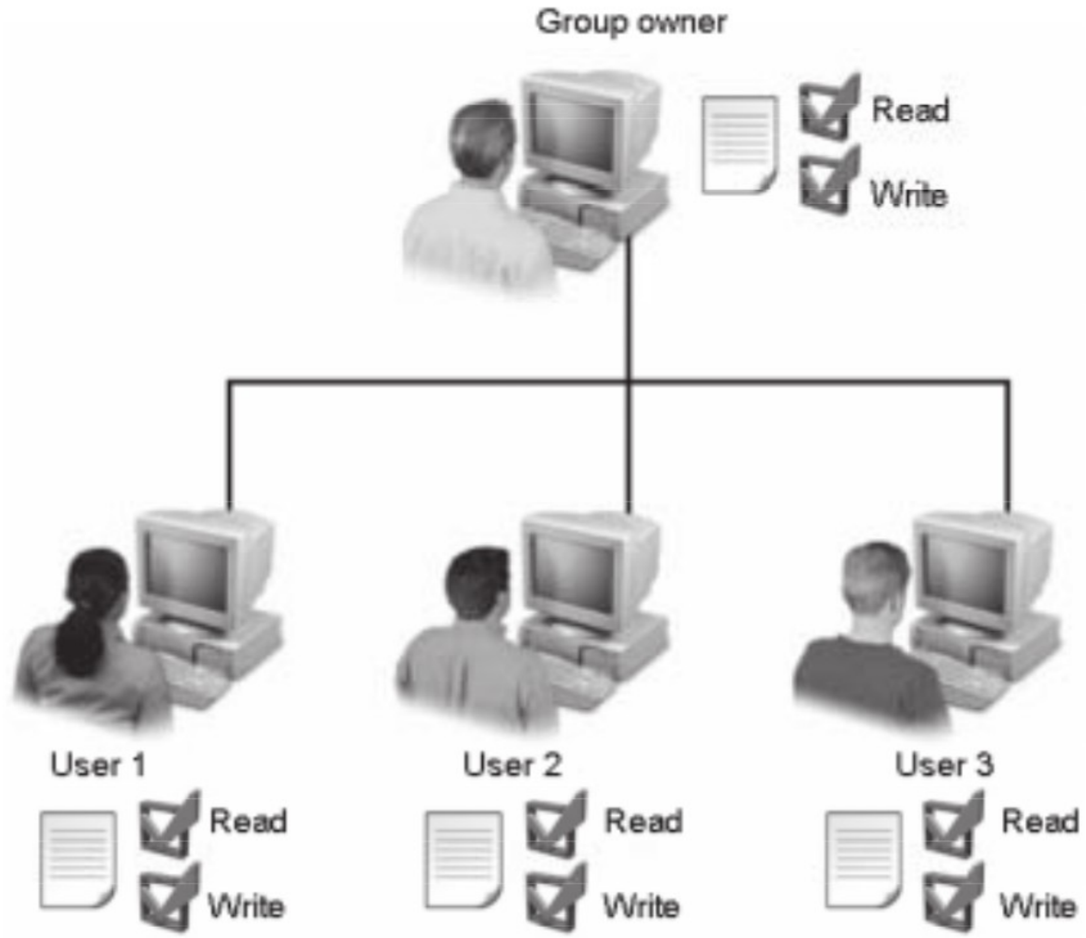
Managing User and Group Accounts

Groups

- A group is a collection of system users having the same access rights. Every user must be a member of a group. Users can also be members of more than one group. Group membership is used to limit access to files and system resources. The groupadd command allows you to add a group.
- The syntax of the groupadd command is *groupadd {group name}*.
- *User Private Groups*
  - *A User Private Group (UPG) is a unique group that is created by default whenever a new user account is created. This is the primary group of the new user account. Only the new user is a member of this group.*

Managing User and Group Accounts

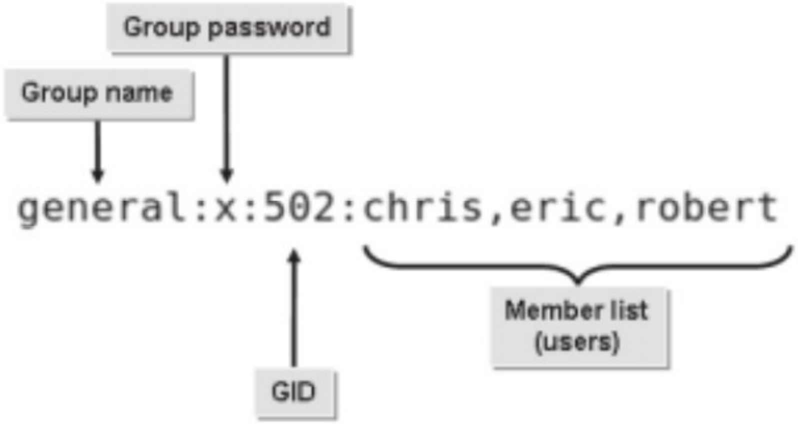
Groups



Managing User and Group Accounts

Groups

- The /etc/group File
  - The /etc/group file contains a list of groups, each on a separate line. Each line consists of four fields for attribute definition, separated by colons. The /etc/group file is also termed as the group database.



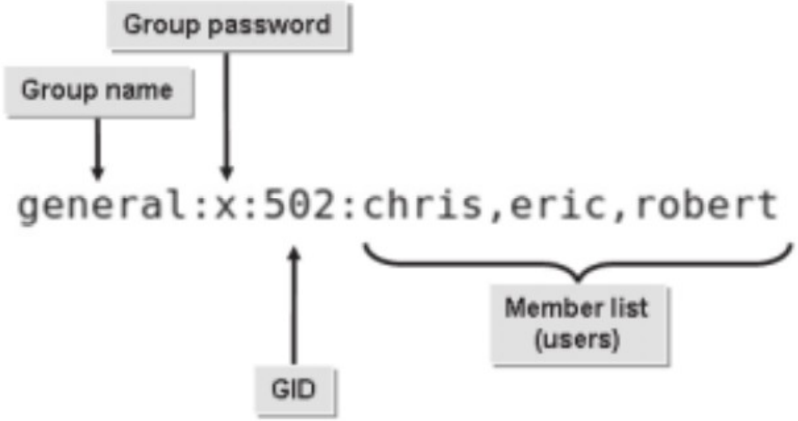
```
general:x:502:chris,eric,robert
```

- The /etc/gpasswd file stores the encrypted passwords for groups.

Managing User and Group Accounts

Groups

- The /etc/group File
  - The /etc/group file contains a list of groups, each on a separate line. Each line consists of four fields for attribute definition, separated by colons. The /etc/group file is also termed as the group database.

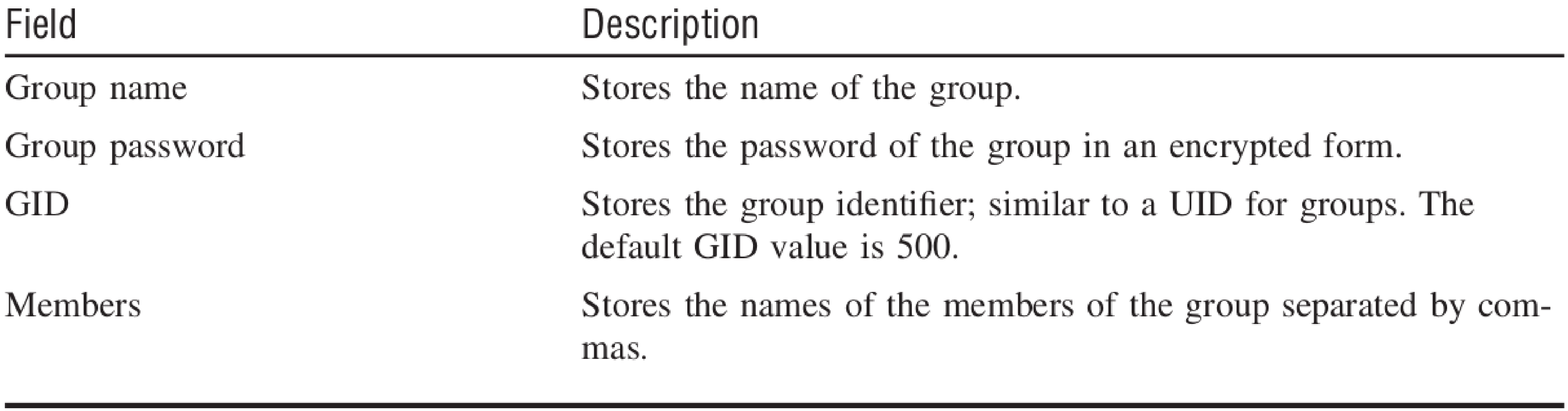


```
general:x:502:chris,eric,robert
```

- The /etc/gpasswd file stores the encrypted passwords for groups.

Managing User and Group Accounts

Groups



Field	Description
Group name	Stores the name of the group.
Group password	Stores the password of the group in an encrypted form.
GID	Stores the group identifier; similar to a UID for groups. The default GID value is 500.
Members	Stores the names of the members of the group separated by commas.

Thanks For Attention