3.9 passwd: CHANGING YOUR PASSWORD

The remaining commands in this chapter relate to our UNIX system, and we'll first take up the command that changes the user's password. In Chapter 1, you have seen how keying in a wrong password prevents you from accessing the system. If your account doesn't have a password or has one that is already known to others, you should change it immediately. This is done with the **passwd** command:

```
$ passwd
passwd:  Changing password for kumar
Enter login password: *******                    Asks for old password
New password: ********
Re-enter new password: ********
passwd (SYSTEM): passwd successfully changed for kumar
```

passwd (note the spelling) expects you to respond three times. First, it prompts for the old password. Next, it checks whether you have entered a valid password, and if you have, it then prompts for the new password. Enter the new password using the password naming rules applicable to your system. Finally, **passwd** asks you to reenter the new password. If everything goes smoothly, the new password is registered by the system.

When you enter a password, the string is *encrypted* by the system. Encryption generates a string of seemingly random characters that UNIX subsequently uses to determine the authenticity of a password. This encryption is stored in a file named shadow in the /etc directory. Even if a user is able to see the encryption in the file, she can't work backwards and derive the original password string from the encryption.

Note: This is the first time you have changed the *state* of the system; you have indirectly modified a file (shadow) *that is otherwise not available to you for direct editing*. There's a special feature of UNIX that allows you to do that, and we'll be examining it at the end of Part I of this text.

3.9.1 Password Framing Rules and Discipline

Depending on the way they are configured, many systems conduct certain checks on the string that you enter as password. There is often a minimum length of the string. Many systems insist on using a mix of letters with numerals. They may either disallow you from framing easy-to-remember passwords or advise you against choosing a bad password. The following messages are quite common:

```
passwd(SYSTEM): Password too short - must be at least 6 characters.
passwd(SYSTEM): Passwords must differ by at least 3 positions.
passwd(SYSTEM): The first 6 characters of the password must contain at least
two alphabetic characters and at least one numeric or special character.
BAD PASSWORD: it is based on a dictionary word.
BAD PASSWORD: is too similar to the old one.
passwd(SYSTEM): Too many failures - try later.
```

These messages suggest that you are not able to choose any password you like. These are some of the rules that you are expected to follow when handling your own password:

- Don't choose a password similar to the old one.
- Don't use commonly used names like names of friends, relatives, pets and so forth. A system may check with its own dictionary and throw out those passwords that are easily guessed.

- Use a mix of alphabetic or numeric characters. Enterprise UNIX systems won't allow passwords that are wholly alphabetic or numeric.
- Don't write down the password in an easily accessible document.
- Change the password regularly.

You must remember your password, but if you still forget it, rush to your system administrator. You'll learn later of the terrible consequences that you may have to face if people with mischievous intent somehow come to know what your password is. The command also behaves differently when used by the system administrator; it doesn't ask for the old password. The **passwd** command is revisited in Chapter 15.