NAME

passwd − password file

DESCRIPTION

Passwd is a text file, that contains a list of the system's accounts, giving for each account some useful information like user ID, group ID, home directory, shell, etc. Often, it also contains the encrypted passwords for each account. It should have general read permission (many utilities, like **ls**(1) use it to map user IDs to usernames), but write access only for the superuser.

In the good old days there was no great problem with this general read permission. Everybody could read the encrypted passwords, but the hardware was too slow to crack a well-chosen password, and moreover, the basic assumption used to be that of a friendly user-community. These days many people run some version of the shadow password suite, where */etc/passwd* has "x" instead of encrypted passwords, and the encrypted passwords are in */etc/shadow* which is readable by the superuser only.

If the encrypted password, whether in /etc/passwd or in /etc/shadow, is an empty string, login is allowed without even asking for a password. Note that this functionality may be intentionally disabled in applications, or configurable (for example using the "nullok" or "nonull" arguments to pam_unix.so).

If the encrypted password in /etc/passwd is "*NP*" (without the quotes), the shadow record should be obtained from a NIS+ server.

Regardless of whether shadow passwords are used, many sysadmins use an asterisk in the encrypted password field to make sure that this user can not authenticate him- or herself using a password. (But see the Notes below.)

If you create a new login, first put an asterisk in the password field, then use **passwd**(1) to set it.

There is one entry per line, and each line has the format:

account:password:UID:GID:GECOS:directory:shell

The field descriptions are:

account the name of the user on the system. It should not contain capital letters.

password the encrypted user password, an asterisk (*), or the letter 'x'. (See **pwconv**(8) for an explanation of 'x'.)

UID the numerical user ID.

GID the numerical primary group ID for this user.

GECOS This field is optional and only used for informational purposes. Usually, it contains the full username. GECOS means General Electric Comprehensive Operating System, which has been renamed to GCOS when GE's large systems division was sold to Honeywell. Dennis Ritchie has reported: "Sometimes we sent printer output or batch jobs to the GCOS machine. The gcos field in the password file was a place to stash the information for the $IDENTcard. Not elegant."

directory the user's **$HOME** directory.

shell the program to run at login (if empty, use */bin/sh*). If set to a non-existing executable, the user will be unable to login through **login**(1).

FILES

/etc/passwd

NOTES

If you want to create user groups, their GIDs must be equal and there must be an entry in */etc/group*, or no group will exist.

If the encrypted password is set to an asterisk, the user will be unable to login using **login**(1), but may still login using **rlogin**(1), run existing processes and initiate new ones through **rsh**(1), **cron**(8), **at**(1), or mail

filters, etc. Trying to lock an account by simply changing the shell field yields the same result and additionally allows the use of **su**(1).

SEE ALSO

login(1), **passwd**(1), **su**(1), **getpwent**(3), **getpwnam**(3), **group**(5), **shadow**(5)

COLOPHON

This page is part of release 3.22 of the Linux *man-pages* project. A description of the project, and information about reporting bugs, can be found at http://www.kernel.org/doc/man-pages/.