Ubuntu Linux Fundamentals

Ubuntu Server - /etc/shadow

The /etc/password file, but itself, cannot perform the function of permitting user login on modern Linux systems. It has to be coupled with the /etc/shadow file.

The /etc/shadow File

The /etc/shadow file, paired with the /etc/passwd file, permits users to log in. The system checks the entered password against the value stored in /etc/shadow, and if it's right, the user is permitted to log in. If not, you can try again. Only a few more times, though if an account lockout is set.

Here's a line from the /etc/shadow file:

```
lskywalker:$6$7AGLK73G$wCV11kWNLz2a/
zWUZH5coRvTKP48VQOluVJo0MHN7SdmQW7JFibGfnYQxP89V3PWXHWDQR5qOmNDnpoIvCn
v./:17473:0:99999:7:::
```

As with the /etc/passwd file, the line is a set of fields separated by colons ":"

1. Username (`lskywalker`).
2. The encrypted password.
The encrypted password consists of the following fields:
a. `$6` - This value could be a number from 1 to 6, and it signifies the encryption level used.
$1 = MD5
$2a = Blowfish
$2y = Blowfish - With correct handling of 8 bit characters
$4 = sha-256
$6 = sha-512
b. `$7AGLK73` - This is the salt (after the $) used to create the encrypted password.
c. `$wCV11kWNLz2azWUZH5coRvTKP48VQOluVJo0MHN7SdmQW7JFibGfnYQxP89V3PWXHWDQR5qOmNDnpoIvCnv./` - The encrypted password
3. Last password change date (days since 1 January 1970). Weird way to calculate it. (`17473` here)
4. Minimum password age (0)
4. Maximum password age (`99999`) ~274 years! In effect, it never expires.
5. Number of days before password expires to warn the user. (`7`)
6. Normally blank, but if filled in, it will indicate the number of days after the password expires until the account is disabled.
7. Expiration - Days from 1 January 1970 that the account will be disabled on. An expiration.

If you look at the file, you'll notice many users with an * in the password field, as in the entry below:

```
games:*:17379:0:99999:7:::
```

For those accounts, the password is not set, so that account cannot be used to log into the system.

Remember, to edit the `/etc/shadow` file, which you probably shouldn't do manually anyway, give yourself a little protection by using the `vipw -s` command.

More Information

BackTrack (now Kali) Linux article explaining the /etc/shadow file
https:://www.backtrack-linux.org/forums/showthread.php?t=39771

NixCraft article on /etc/shadow
https://www.cyberciti.biz/faq/understanding-etcshadow-file/