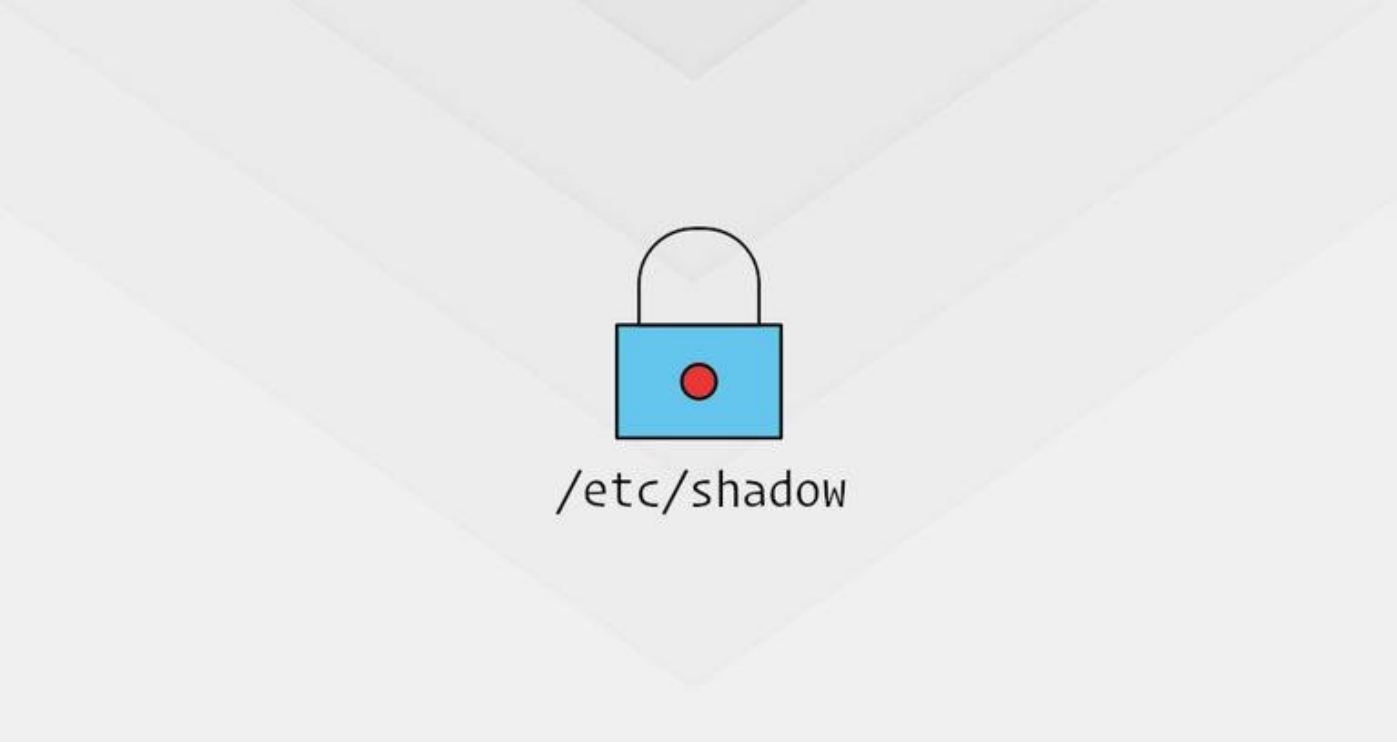
Understanding the /etc/shadow File

Posted Dec 27, 2019 • 4 min read



There are several different authentication schemes that can be used on Linux systems. The most commonly used and standard scheme is to perform authentication against the `/etc/passwd` and `/etc/shadow` files.

`/etc/shadow` is a text file that contains information about the system's users' passwords. It is owned by user root and group shadow, and has 640 permissions .

`/etc/shadow` Format

The `/etc/shadow` file contains one entry per line, each representing a user account. You can view the contents of the file, with a text editor or a command such as `cat` :

```
$ sudo cat /etc/shadow
```

user accounts. New entries are appended at the end of the file.

Each line of the `/etc/shadow` file contains nine comma-separated fields:

```
mark:$6$.n.:17736:0:99999:7:::
[--] [----] [---] - [---] ----
|      |      |   |   |   |||+-----------> 9. Unused
|      |      |   |   |   ||+------------> 8. Expiration date
|      |      |   |   |   |+-------------> 7. Inactivity period
|      |      |   |   |   +--------------> 6. Warning period
|      |      |   |   +------------------> 5. Maximum password age
|      |      |   +----------------------> 4. Minimum password age
|      |      +--------------------------> 3. Last password change
|      +---------------------------------> 2. Encrypted Password
+------------------------------------------> 1. Username
```

01. Username. The string you type when you log into the system. The user account that exist on the system.

02. Encrypted Password. The password is using the `$type$salt$hashed` format. `$type` is the method cryptographic hash algorithm and can have the following values:

    - `$1$` – MD5
    - `$2a$` – Blowfish
    - `$2y$` – Eksblowfish
    - `$5$` – SHA-256
    - `$6$` – SHA-512

    If the password field contains an asterisk (`*`) or exclamation point (`!`), the user will not be able to login to the system using password authentication. Other login methods like key-based authentication or switching to the user are still allowed.

    In older Linux systems, the user's encrypted password was stored in the

03. Last password change. This is the date when the password was last changed. The number of days is counted since January 1, 1970 (epoch date).

04. Minimum password age. The number of days that must pass before the user password can be changed. Typically it is set to zero, which means that there is no minimum password age.

05. Maximum password age. The number of days after the user password must be changed. By default, this number is set to `99999`.

06. Warning period. The number of days before the password expires during which the user is warned that the password must be changed.

07. Inactivity period. The number of days after the user password expires before the user account is disabled. Typically this field is empty.

08. Expiration date. The date when the account was disabled. It is represented as an epoch date.

09. Unused. This field is ignored. It is reserved for future use.

The `/etc/shadow` file should not be edited by hand unless you know what you are doing. Always use a command that is designed for the purpose. For example, to change a user password, use the `passwd` command, and to change the password aging information, use the `chage` command.

Let’s take a look at the following example:

```
linuxize:$6$zHvrJMa5Y690smbQ$z5zdL...:18009:0:120:7:14::
```

The entry above contains information about the user “linuxize” password:

- The password is encrypted with SHA-512 (the password is truncated for better readability).
- The password was last changed on April 23, 2019 - `18009` .
- There is no minimum password age.
- The password must be changed at least every 120 days.
- The user will receive a warning message seven days before the password expiration date.
- If the user doesn’t attempt to login to the system 14 days after the password is expired, the account will be disabled.
- There is no account expiration date.

Conclusion

The `/etc/shadow` file keeps records about encrypted users' passwords, as well as other passwords related information.

If you have any questions or feedback, feel free to leave a comment.

terminal