Understanding Shadow File Format in Linux

719 Rakhi June 27, 2024 General 848

Understanding the format of /etc/shadow file

The **/etc/shadow** file also named the shadow password file is an important part of Linux systems, as it is designed to store user password information securely. The password stored in the shadow file is in an encrypted manner and is accessible only to root users, preventing unauthorized access from breaking into the system. Traditional password files are maintained in **/etc/passwd**, but the actual hashed passwords are stored in **/etc/shadow**. Each line in this file represents a user account and includes multiple fields separated by colons (:).

- **Permissions in /etc/shadow file.**

The default permission for the **/etc/shadow** file is -rw-r----- which translates to the numeric permission 640.

- ***Owner*** *(root)*: read and write (rw-)
- ***Group*** *(shadow):* read (r--)
- ***Others***: no permissions (---)

In numeric form, these permissions would mean as follows:

- 6 for owner (4 for read + 2 for write)
- 4 for group (4 for read)
- 0 for others (no permissions)

It is crucial that these permissions are strictly maintained to prevent unauthorized access to sensitive password data.

```
:~# ls -l /etc/shadow
-rw-r----- 1 root shadow 2490 Jun 13 03:39 /etc/shadow
```

- **Format of /etc/shadow file.**

The standard format for each line is:

```
root@gateway:~# grep tom /etc/shadow
tom:$6$rounds=5299$5JhMYd9kZZRti5Ap$9qrU1uwmCFu0MOsuGY7IljlHUAS1O70vNjQ07L.qqDtQE/zM0sgiLgf30sRR5/r4AS5.gzIzIu/Xdxf.GWmj8/:19887:0:99999:7:::
root@gateway:~#
```

SYNTAX: username:password:lastchanged:min:max:warn:inactive:expire:reserved

```
tom:$6$.n.:19887:0:99999:7:::
[--] [----] [---] - [---] ----
| | | | | |||+-----------> 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
```

The **/etc/shadow** file contains the following information:

1. Username: It must be a valid account name, which exists on the system.

2. Encrypted Password: This field may be empty, in which case no passwords are required to authenticate as the specified login name. However, some applications that read the /etc/shadow file may decide not to permit any access at all if the password field is empty. A password field that starts with an exclamation mark means that the password is locked. The remaining characters on the line represent the password field before the password was locked. Refer to crypt(3) for details on how this string is interpreted if the password field contains some string that is not a valid result of crypt(3), for instance! or *, the user will not be able to use a Unix password to log in (but the user may log in to the system by other means).

3. Date of last password change: The date of the last password change, expressed as the number of days since Jan 1, 1970, 00:00 UTC. The value 0 has a special meaning, which is that the user should change her password the next time she logs in to the system. An empty field means that password aging features are disabled.

4. Minimum password age: The minimum password age is the number of days the user will have to wait before she will be allowed to change her password again. An empty field and a value of 0 means that there is no minimum password age.

5. Maximum password age: The maximum password age is the number of days after which

the user will have to change her password. After this number of days has elapsed, the password may still be valid. The user should be asked to change her password the next time she logs in. An empty field means that there is no maximum password age, no password warning period, and no password inactivity period (see below). If the maximum password age is lower than the minimum password age, the user cannot change her password.

6. Password warning period: The number of days before a password is going to expire (see the maximum password age above) during which the user should be warned. An empty field and a value 0 mean that there is no password warning period.

7. Password inactivity period: The number of days after a password has expired (see the maximum password age above) during which the password should still be accepted (and the user should update her password during the next login). After the expiration of the password and this expiration period has elapsed, no login is possible for the user. The user should contact her administrator. An empty field means that there is no enforcement of an inactivity period.

8. Account expiration date: The date of expiration of the account, expressed as the number of days since Jan 1, 1970, 00:00 UTC. Note that an account expiration differs from a password expiration. In case of an account expiration, the user shall not be allowed to log in. In case of a password expiration, the user is not allowed to log in using her password. An empty field means that the account will never expire. The value 0 should not be used as it is interpreted as either an account with no expiration or as an expiration on Jan 1, 1970.

9. Reserved field: This field is reserved for future use.

Related Articles:

Setup Ezeelogin Jump Server

Where is the password of the user stored

Different password management options in ezeelogin