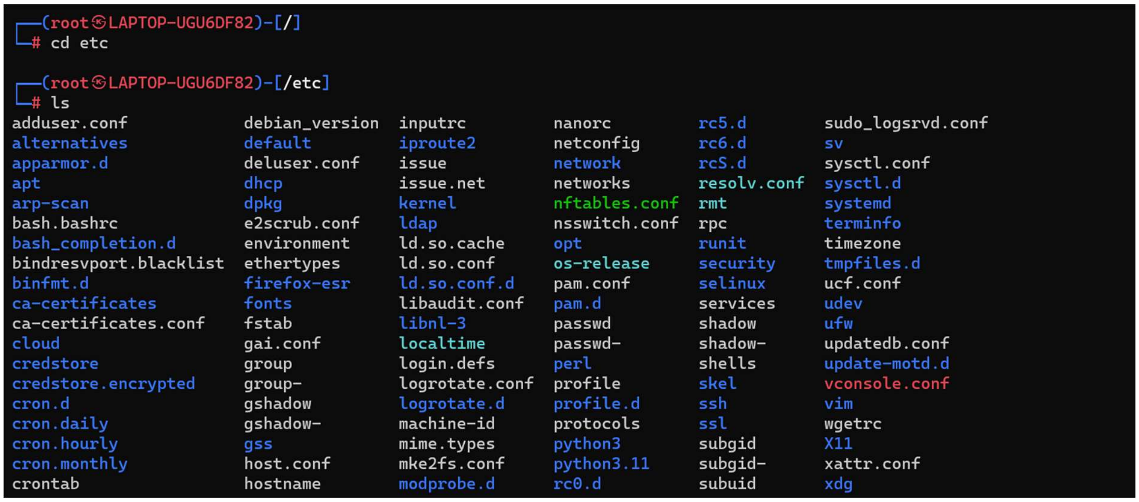
# Task 3 # /etc/shadow and /etc/passwd in linux

Name :Deep Salunkhe

Roll No: 21102A0014

Div: TE CMPN A

In Linux, **/etc/passwd** and **/etc/shadow** are two important system files used for user account management and authentication.

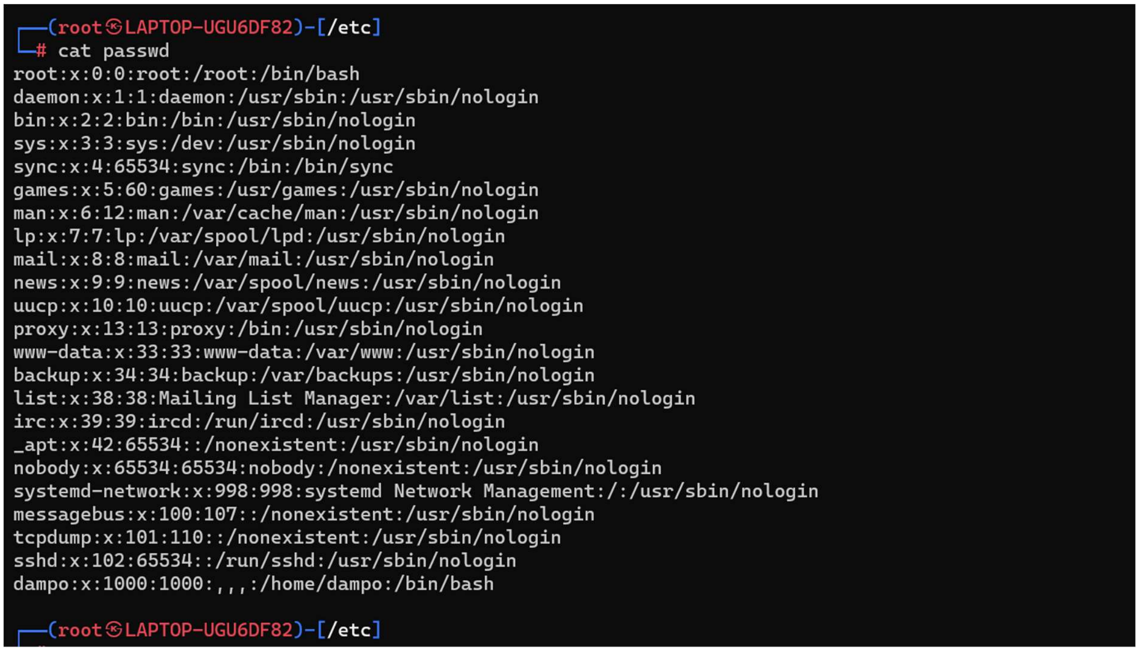


```
┌──(root㉿LAPTOP-UGU6DF82)-[/]
└─# cd etc

┌──(root㉿LAPTOP-UGU6DF82)-[/etc]
└─# ls
adduser.conf            debian_version  inputrc         nanorc         rc5.d        sudo_logsrvd.conf
alternatives            default         iproute2        netconfig      rc6.d        sv
apparmor.d              deluser.conf    issue           network        rcS.d        sysctl.conf
apt                     dhcp            issue.net       networks       resolv.conf  sysctl.d
arp-scan                dpkg            kernel          nftables.conf  rmt          systemd
bash.bashrc             e2scrub.conf    ldap            nsswitch.conf  rpc          terminfo
bash_completion.d       environment     ld.so.cache     opt            runit        timezone
bindresvport.blacklist  ethertypes      ld.so.conf      os-release     security     tmpfiles.d
binfmt.d                firefox-esr     ld.so.conf.d    pam.conf       selinux      ucf.conf
ca-certificates         fonts           libaudit.conf   pam.d          services     udev
ca-certificates.conf    fstab           libnl-3         passwd         shadow       ufw
cloud                   gai.conf        localtime       passwd-        shadow-      updatedb.conf
credstore               group           login.defs      perl           shells       update-motd.d
credstore.encrypted     group-          logrotate.conf  profile        skel         vconsole.conf
cron.d                  gshadow         logrotate.d     profile.d      ssh          vim
cron.daily              gshadow-        machine-id      protocols      ssl          wgetrc
cron.hourly             gss             mime.types      python3        subgid       X11
cron.monthly            host.conf       mke2fs.conf     python3.11     subgid-      xattr.conf
crontab                 hostname        modprobe.d      rc0.d          subuid       xdg
```

**/etc/passwd:**

- This file contains user account information, including usernames, user IDs (UIDs), group IDs (GIDs), home directories, and default shells.
  - **username**: The name of the user.
  - **password**: The user's password, represented by a placeholder (such as **x**). Historically, the actual encrypted password was stored here, but modern systems store password hashes in **/etc/shadow**.
  - **UID**: The user's unique numerical identifier.
  - **GID**: The primary group ID of the user.
  - **GECOS**: Additional user information, typically including the user's full name.
  - **home_directory**: The user's home directory.
  - **shell**: The user's default shell.

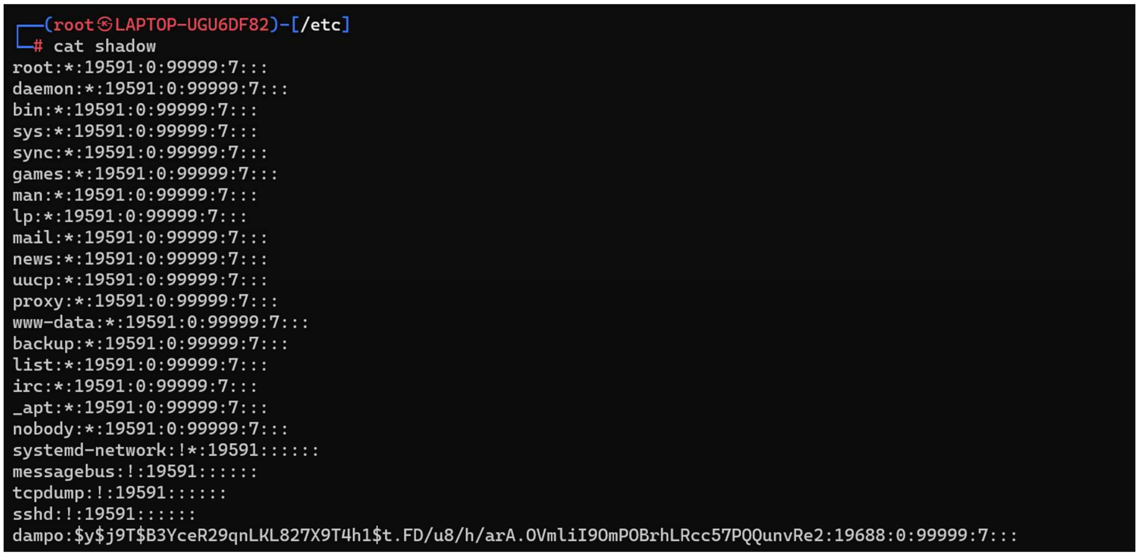


```
┌──(root㉿LAPTOP-UGU6DF82)-[/etc]
└─# cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
messagebus:x:100:107::/nonexistent:/usr/sbin/nologin
tcpdump:x:101:110::/nonexistent:/usr/sbin/nologin
sshd:x:102:65534::/run/sshd:/usr/sbin/nologin
dampo:x:1000:1000:,,,:/home/dampo:/bin/bash

┌──(root㉿LAPTOP-UGU6DF82)-[/etc]
```

**/etc/shadow:**

- This file contains the encrypted password hashes and related password information for user accounts.
- The **/etc/shadow** file is typically only readable by the root user (**root**), providing an additional layer of security.
    - **username**: The name of the user.
    - **password**: The hashed password. On modern systems, this is typically a password hash generated using a cryptographic hash function (such as SHA-256 or bcrypt).
    - **last_password_change**: The date of the last password change, represented in days since the Unix epoch (January 1, 1970).
    - **min_days**: The minimum number of days required between password changes.
    - **max_days**: The maximum number of days the password is valid before expiration.
    - **warn_days**: The number of days before password expiration to display a warning to the user.
    - **inactive_days**: The number of days after password expiration before the account is disabled.
    - **expiration_date**: The expiration date of the account, represented in days since the Unix epoch.
    - **reserved**: Reserved field for future use.



```
┌──(root㉿LAPTOP-UGU6DF82)-[/etc]
└─# cat shadow
root:*:19591:0:99999:7:::
daemon:*:19591:0:99999:7:::
bin:*:19591:0:99999:7:::
sys:*:19591:0:99999:7:::
sync:*:19591:0:99999:7:::
games:*:19591:0:99999:7:::
man:*:19591:0:99999:7:::
lp:*:19591:0:99999:7:::
mail:*:19591:0:99999:7:::
news:*:19591:0:99999:7:::
uucp:*:19591:0:99999:7:::
proxy:*:19591:0:99999:7:::
www-data:*:19591:0:99999:7:::
backup:*:19591:0:99999:7:::
list:*:19591:0:99999:7:::
irc:*:19591:0:99999:7:::
_apt:*:19591:0:99999:7:::
nobody:*:19591:0:99999:7:::
systemd-network:!*:19591::::::
messagebus:!:19591::::::
tcpdump:!:19591::::::
sshd:!:19591::::::
dampo:$y$j9T$B3YceR29qnLKL827X9T4h1$t.FD/u8/h/arA.OVmliI90mPOBrhLRcc57PQQunvRe2:19688:0:99999:7:::
```

## #Difference between these two files

1. **Purpose:**
   - **/etc/passwd**: It stores basic user account information, including usernames, user IDs (UIDs), group IDs (GIDs), home directories, and default shells.
   - **/etc/shadow**: It stores encrypted password hashes and related password policies for user accounts, providing an additional layer of security.
2. **Accessibility:**
   - **/etc/passwd**: This file is readable by all users on the system. It contains non-sensitive information about user accounts.
   - **/etc/shadow**: This file is typically only readable by the root user (**root**). It contains sensitive information such as encrypted password hashes and password-related policies.
3. **Contents:**
   - **/etc/passwd**: Each line in this file represents a user account and includes fields such as username, password (historically), UID, GID, GECOS, home directory, and default shell.
   - **/etc/shadow**: Each line in this file also represents a user account but includes fields such as username, encrypted password hash, last password change date, minimum and maximum password age, and other password-related information.
4. **Password Storage:**

- **/etc/passwd**: Historically, this file stored the actual encrypted passwords of user accounts. However, modern Linux systems store password hashes in **/etc/shadow**.
- **/etc/shadow**: This file stores the encrypted password hashes generated using cryptographic hash functions like SHA-256 or bcrypt. Storing password hashes instead of plaintext passwords enhances security by protecting against password disclosure.

5. **Security:**
    - **/etc/passwd**: Since it contains non-sensitive information and is readable by all users, **/etc/passwd** poses a lower security risk.
    - **/etc/shadow**: This file contains sensitive information such as password hashes and password-related policies. Access to **/etc/shadow** is restricted to the root user (**root**) to prevent unauthorized access and protect against password-related security breaches.
6. **User Authentication:**
    - **/etc/passwd**: Historically, the password field in **/etc/passwd** contained the encrypted passwords. However, modern systems use **/etc/shadow** for storing password hashes and related policies, making **/etc/passwd** less relevant for user authentication.
    - **/etc/shadow**: This file is crucial for user authentication on Linux systems. It stores encrypted password hashes, enforcing password policies such as minimum and maximum password age, expiration dates, and account lockout.
7. **File Permissions:**
    - **/etc/passwd**: Typically, this file has permissions set to **644** (**-rw-r--r--**), allowing read access for all users and write access only for the root user (**root**).
    - **/etc/shadow**: This file has strict permissions set to **640** (**-rw-r-----**), allowing read and write access only for the root user (**root**) and read access for the group members of **shadow**.
8. **File Format:**
    - **/etc/passwd**: Each line in **/etc/passwd** is structured with fields separated by colons (**:**). These fields include username, password (historically), UID, GID, GECOS, home directory, and default shell.
    - **/etc/shadow**: Similar to **/etc/passwd**, each line in **/etc/shadow** is structured with fields separated by colons (**:**). These fields include username, encrypted password hash, last password change date, minimum and maximum password age, warning period, inactivity period, expiration date, and a reserved field.
9. **Historical Significance:**

- **/etc/passwd**: Historically, **/etc/passwd** stored encrypted passwords. However, this practice posed security risks, leading to the creation of **/etc/shadow** for more secure password storage.
- **/etc/shadow**: Introduced as a security enhancement, **/etc/shadow** securely stores password hashes and password-related policies, reducing the risk of password compromise.

10. **Usage in Authentication Process:**
    - **/etc/passwd**: In the past, **/etc/passwd** was used directly for authentication, with the password field containing encrypted passwords. However, modern systems use **/etc/shadow** for authentication, with **/etc/passwd** mainly used for user account information.
    - **/etc/shadow**: It plays a critical role in the authentication process, storing password hashes and enforcing password policies, such as password expiration and account locking.
11. **Compatibility:**
    - **/etc/passwd**: The format and content of **/etc/passwd** are relatively stable across different Unix-like operating systems (e.g., Linux, Unix, macOS).
    - **/etc/shadow**: The presence and format of **/etc/shadow** may vary across different Unix-like operating systems. While most Linux distributions use **/etc/shadow** for password storage, some Unix variants may use alternative methods.
12. **Backup and Recovery:**
    - **/etc/passwd**: Since it contains non-sensitive user information, backup and recovery procedures for **/etc/passwd** are straightforward and do not involve handling sensitive data.
    - **/etc/shadow**: Due to its sensitive nature, backup and recovery procedures for **/etc/shadow** require careful handling to prevent unauthorized access to password hashes and related information.
13. **Logging and Auditing:**
    - **/etc/passwd**: Changes to **/etc/passwd** (e.g., user additions, modifications) may be logged for auditing purposes, depending on system configuration.
    - **/etc/shadow**: Access to **/etc/shadow** and changes made to password-related information are often logged for auditing and security analysis, helping administrators track unauthorized access attempts and enforce security policies.