This is **Lab 6 of the Cisco NetAcad & LPI Linux Essentials learning path: System and User Security**. By performing this lab, students will be able to monitor who has been attempting to log in to the system, and view user and group permissions.

In this lab, I will perform the following tasks:

- Learn the difference between the superuser account and regular user accounts.
- View user account information.

Administrative user

In this task, I will learn two ways to run commands as an administrative user. This is often necessary for making changes that affect the whole system.

To access the root user account, the su or sudo commands are normally used.

The su command is usually used to switch users and start a new shell as another user, with the default being the root user. The su command is often used when a *series of commands* need to be executed as the root user.

The sudo command is typically used to execute a *single command* as the root user by prefixing that command with sudo. The sudo command must be configured by the root user before an ordinary user can use it. By default, the sudo command stays in effect for 15 minutes on Ubuntu systems where the root account is *not* enabled by default. Root access has been enabled on the virtual machine used in this lab allowing the su command to be used.

Step 1

Switch users to the root user and provide the root password of netlab123 when prompted. Confirm the new user identity using the id command.

Step 2

After using the shell started by the su command to perform the necessary administrative tasks, return to your original shell (and original user account) by using the exit command. Confirm the user identity change using the id command.

Step 3

Type head /etc/shadow without sudo permissions. Now retype the same command using sudo

```
sysadmin@localhost:~$ su
Password:
root@localhost:~# id
uid=0(root) gid=0(root) groups=0(root)
root@localhost:~# exit
exit
sysadmin@localhost:~$ id
uid=1001(sysadmin) gid=1001(sysadmin) groups=1001(sysadmin),4(adm),27(sudo)
sysadmin@localhost:~$ head /etc/shadow
head: cannot open '/etc/shadow' for reading: Permission denied
sysadmin@localhost:~$ sudo head /etc/shadow
[sudo] password for sysadmin:
root:$6$HHJ0w8Vo$qBlf7KzplwMRKqa7DGAV3LywgVypyiDuxewwMfHy6GTEEa7IvIiQndL9Bkp4ixR
PjrjBr1rkZuFC60oRbX4Rq0:18666:0:99999:7:::
daemon:*:18645:0:99999:7:::
bin:*:18645:0:99999:7:::
sys:*:18645:0:99999:7:::
sync:*:18645:0:99999:7:::
games:*:18645:0:99999:7:::
man:*:18645:0:99999:7:::
lp:*:18645:0:99999:7:::
mail:*:18645:0:99999:7:::
news:*:18645:0:99999:7:::
sysadmin@localhost:~$
```

User Accounts

In this task, I will learn about user accounts and the files and commands that display user account information.

Step 1

User and system accounts are defined in the /etc/passwd and /etc/shadow files. View the first ten lines from the /etc/passwd file. While the passwd file contains general information about a user such as username, UID, GID, home directory and login shell, the modern shadow file has additional details including encrypted password and password policy.

Step 2

Use the grep command to view the record for your sysadmin account. By using the grep command, the output only includes the account information for that one username.

```
sysadmin@localhost:~$ head /etc/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
sysadmin@localhost:~$ grep sysadmin /etc/passwd
sysadmin:x:1001:1001:System Administrator,,,,:/home/sysadmin:/bin/bash
sysadmin@localhost:~$
```

Passwords

The /etc/shadow file contains information about users' passwords. In this exercise I will use several commands to view the data in this file.

Step 1

Try to view the first few lines of /etc/shadow file, a file that contains users' encrypted passwords and information about aging them.

Step 2

Notice that the permissions on the /etc/shadow file indicate that only members of the shadow group have permission to view the file

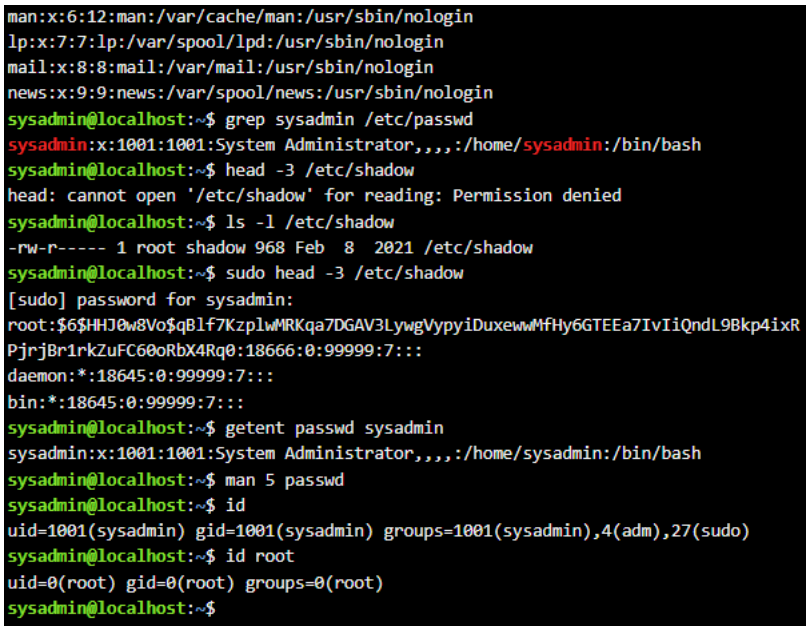
Step 3

Use the sudo command to view the first few lines of the /etc/shadow file. Provide the password of the sysadmin user, netlab123, when prompted. Step 4

Another way to retrieve the account information for a user is by running the following command: getent passwd *username*. The getent command has the advantage over the grep command as it is also able to access user accounts that are not defined locally. In other words, the getent command is able to get user information for users who may be defined on network directory servers such as LDAP, NIS, Windows Domain, or Active Directory Domain servers.

Step 4

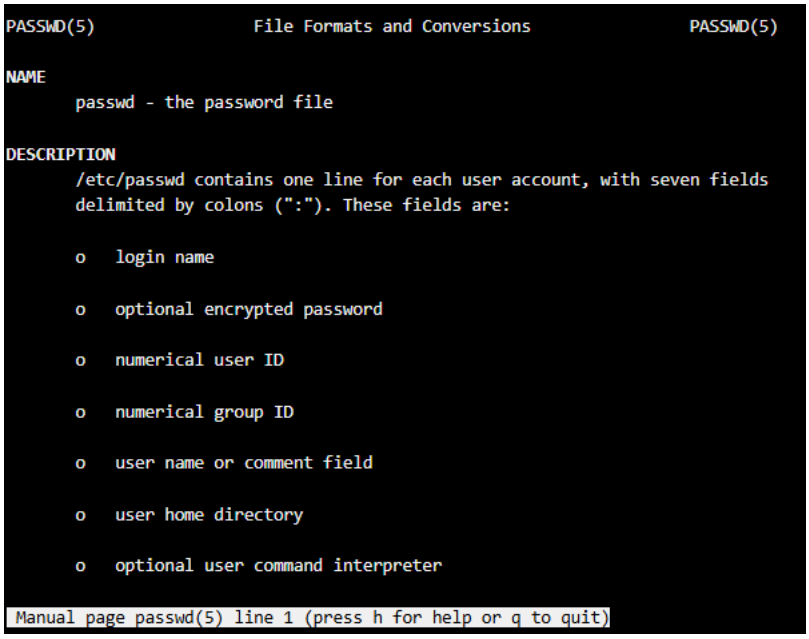
Use the getent command to retrieve the information about the sysadmin



Step 5

You can view the documentation of the fields in the /etc/passwd file with the following command:

man 5 passwd.



Step 6

You can view account information for your account, or a specified user account, using the id command.

Who is On the System

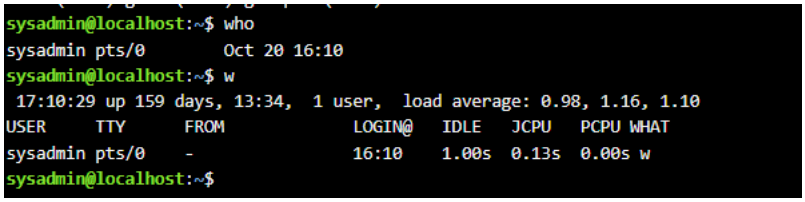
In this task, you will execute some commands to see who is logged into the system.

Step 1

Use the who command to get the current list of users on the system

Step 2

Use the w command to get a more detailed view of the users who are currently on your system.

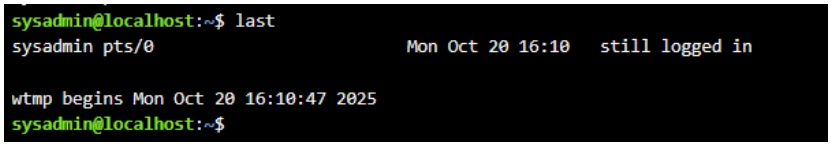


Viewing Login History

The last command reads the entire login history from the /var/log/wtmp file and displays all logins and reboot records by default.

Step 1

Use the last command to view the /var/log/wtmp file which keeps a log of all users who have logged in and out the system.


sysadmin@localhost:~$ last
sysadmin pts/0 Mon Oct 20 16:10 still logged in
wtmp begins Mon Oct 20 16:10:47 2025
sysadmin@localhost:~$