# **Lab 13: System and User Security**

## 13.1 Introduction

This is Lab 13: 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, you will perform the following tasks:

* Learn the difference between the superuser account and regular user accounts.
* View user account information.
* [Previous](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/)
* [Next](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.2)

## 13.2 Running Commands as an Administrator

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

* [Previous](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.1)
* [Next](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.2.1)

## 13.2.1 Step 1

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 13 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.

When executed without arguments, the su command opens a new shell as the root user. There is some confusion as to what the initials “su” stand for (substitute user, switch user, and superuser are all often referenced) , but the main thing to note is that it allows an administrator to change their login to any user on the system.

When entering this command without a username, the system will assume the root user. Most systems will display the current user at the command prompt, but it can be helpful to confirm what user is logged in with the id command as shown below. This step will ensure changes required for specific users (such as service accounts) are executed properly.

Switch users to the root user and provide the root password of netlab123 when prompted:

su -

**sysadmin@localhost:~$** su -

Password:

Confirm the new user identity using the id command:

id

**root@localhost:~#** id

uid=0(root) gid=0(root) groups=0(root)

* [Previous](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.2)
* [Next](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.2.2)

## 13.2.2 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.

exit

id

**root@localhost:~#** exit

logout

**sysadmin@localhost:~$** id

uid=1001(sysadmin) gid=1001(sysadmin) groups=1001(sysadmin),4(adm),27(sudo)

Exiting the shell is important to avoid executing commands as root that could damage the system.

* [Previous](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.2.1)
* [Next](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.2.3)

## 13.2.3 Step 3

The sudo command works on systems that do not allow root access by default. It is preferred for most administrative tasks since root access times out automatically without having to exit. First type a command as the sysadmin non-privileged user.

head /etc/shadow

**sysadmin@localhost:~$** head /etc/shadow

head: cannot open `/etc/shadow' for reading: Permission denied

Notice the error message that the head command displays. This is because the sysadmin user has no rights to view this file. The root user, however, can display this file.

* [Previous](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.2.2)
* [Next](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.2.4)

## 13.2.4 Step 4

Type the same command using sudo. Use the netlab123 password when prompted:

sudo head /etc/shadow

**sysadmin@localhost:~$** sudo head /etc/shadow

[sudo] password for sysadmin:

root:$6$4Yga95H9$8HbxqsMEIBTZ0YomlMffYCV9VE1SQ4T2H3SHXw41M02SQtfAdDVE9mqGp2hr20q

.ZuncJpLyWkYwQdKlSJyS8.:16464:0:99999:7:::

daemon:\*:16463:0:99999:7:::

bin:\*:16463:0:99999:7:::

sys:\*:16463:0:99999:7:::

sync:\*:16463:0:99999:7:::

games:\*:16463:0:99999:7:::

man:\*:16463:0:99999:7:::

lp:\*:16463:0:99999:7:::

mail:\*:16463:0:99999:7:::

news:\*:16463:0:99999:7:::

sysadmin@localhost:~$

The system will prompt for the current user's password, not the root password. If the current user is part of the sudo group, the command will be executed.

By default on many Ubuntu systems, sudo commands entered after the first sudo command will be executed as root without being prompted for a password for the next 13 minutes. Other systems may have different timeouts.

* [Previous](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.2.3)
* [Next](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.3)

## 13.3 User Accounts

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

* [Previous](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.2.4)
* [Next](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.3.1)

## 13.3.1 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:

head /etc/passwd

**sysadmin@localhost:~$** head /etc/passwd

root:x:0:0:root:/root:/bin/bash

daemon:x:1:1:daemon:/usr/sbin:/bin/sh

bin:x:2:2:bin:/bin:/bin/sh

sys:x:3:3:sys:/dev:/bin/sh

sync:x:4:65534:sync:/bin:/bin/sync

games:x:5:60:games:/usr/games:/bin/sh

man:x:6:12:man:/var/cache/man:/bin/sh

lp:x:7:7:lp:/var/spool/lpd:/bin/sh

mail:x:8:8:mail:/var/mail:/bin/sh

news:x:9:9:news:/var/spool/news:/bin/sh

Notice that this file contains a colon delimited database of all user and system accounts available on this system.

User accounts are assigned to users, to allow them access to the operating system. The sysadmin account that you used to log in to the system is a typical user account.

System accounts are used by the operating system or services running processes on it to perform background functions. These accounts often need access to hardware or system files that normally would only be available to the root user. The default permissions for these accounts normally give access to just the sensitive areas needed rather than the broad access of a root or administrator account, thereby limiting the damage that a compromised service account could cause. System accounts are never used directly by regular users.

* [Previous](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.3)
* [Next](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.3.2)

## 13.3.2 Step 2

Use the grep command to view the record for your sysadmin account:

grep sysadmin /etc/passwd

**sysadmin@localhost:~$** grep sysadmin /etc/passwd

**sysadmin**:x:1001:1001:System Administrator,,,,:/home/**sysadmin**:/bin/bash

By using the grep command, the output only includes the account information for that one username.

* [Previous](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.3.1)
* [Next](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.4)

## 13.4 Passwords

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

* [Previous](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.3.2)
* [Next](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.4.1)

## 13.4.1 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:

head -3 /etc/shadow

**sysadmin@localhost:~$** head -3 /etc/shadow

head: cannot open `/etc/shadow' for reading: Permission denied

**sysadmin@localhost:~$**

Notice the error message that the head command displays. This is because the sysadmin user has no rights to view this file. The root user, however, can display this file.

* [Previous](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.4)
* [Next](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.4.2)

## 13.4.2 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:

ls -l /etc/shadow

**sysadmin@localhost:~$** ls -l /etc/shadow

-rw-r----- 1 root shadow 838 Mar 14 17:34 /etc/shadow

**sysadmin@localhost:~$**

Keep in mind that the root user can view any file. This is due to the root account having special privileges that transcend regular file permissions.

* [Previous](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.4.1)
* [Next](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.4.3)

## 13.4.3 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.

sudo head -3 /etc/shadow

**sysadmin@localhost:~$** sudo head -3 /etc/shadow

[sudo] password for sysadmin:

root:$6$T3W2rbrt$N/2Jrt1EzQ8TqOvxWkYjEpIf3tCbPOyFwU7ZYkToosXB4AGmtb0.W6f8Gb7Vmihnj76yZezNPwMbTGoQFs5Kx1:16874:0:99999:7:::

daemon:\*:16863:0:99999:7:::

bin:\*:16863:0:99999:7:::

**sysadmin@localhost:~$**

**Important**

The password that you provided was for your sysadmin account, not the root account. Once sudo has been configured for your account, you don't need to know the root password to run sudo commands as the root user.

* [Previous](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.4.2)
* [Next](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.4.4)

## 13.4.4 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.

Use the getent command to retrieve the information about the sysadmin:

getent passwd sysadmin

**sysadmin@localhost:~$** getent passwd sysadmin

sysadmin:x:1001:1001:System Administrator,,,,:/home/sysadmin:/bin/bash

**sysadmin@localhost:~$**

**Note**

In this case, we don't have any network accounts, so the output displayed is just like looking at the /etc/passwd file.

The colon delimited /etc/passwd file has the following fields:

name:password:UID:GID:Comment:directory:shell

A breakdown of these fields:

* **Name**

sysadmin:x:1001:1001:System Administrator,,,,:/home/sysadmin:/bin/bash

* **Password Placeholder**

sysadmin:x:1001:1001:System Administrator,,,,:/home/sysadmin:/bin/bash

* **User ID**

sysadmin:x:1001:1001:System Administrator,,,,:/home/sysadmin:/bin/bash

* **Primary Group ID**

sysadmin:x:1001:1001:System Administrator,,,,:/home/sysadmin:/bin/bash

* **Comment**

sysadmin:x:1001:1001:System Administrator,,,,:/home/sysadmin:/bin/bash

* **Home Directory**

sysadmin:x:1001:1001:System Administrator,,,,:/home/sysadmin:/bin/bash

* **Shell**

sysadmin:x:1001:1001:System Administrator,,,,:/home/sysadmin:/bin/bash

* [Previous](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.4.3)
* [Next](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.4.5)

## 13.4.5 Step 5

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

man 5 passwd

PASSWD(5) File Formats and Conversions PASSWD(5)

NAME

passwd - the password file

DESCRIPTION

/etc/passwd contains one line for each user account, with seven fields

delimited by colons (":"). These fields are:

o login name

o optional encrypted password

o numerical user ID

o numerical group ID

o user name or comment field

o user home directory

o optional user command interpreter

**Important**

Remember while viewing a man page, press **Enter** to move forward line by line, **Space** page by page and **q** to quit.

* [Previous](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.4.4)
* [Next](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.4.6)

## 13.4.6 Step 6

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

id

id root

**sysadmin@localhost:~$** id

uid=1001(sysadmin) gid=1001(sysadmin) groups=1001(sysadmin),4(adm),27(sudo)

**sysadmin@localhost:~$** id root

uid=0(root) gid=0(root) groups=0(root)

**sysadmin@localhost:~$**

The output of the commands shows the following:

User identity:

uid=1001(sysadmin) gid=1001(sysadmin) groups=1001(sysadmin),4(adm),27(sudo)

Primary group identity:

uid=1001(sysadmin) gid=1001(sysadmin) groups=1001(sysadmin),4(adm),27(sudo)

Groups that you belong to:

uid=1001(sysadmin) gid=1001(sysadmin) groups=1001(sysadmin),4(adm),27(sudo)

In this case, your user account only belongs to three groups.

**Note**

The file /etc/group, together with /etc/passwd, determines your group memberships. Your default primary group is determined by matching your GID found in /etc/passwd to the GID defined for a group in the /etc/group. Any secondary group memberships are defined in the /etc/group file.

The format of entries in the /etc/group file for each line is:

group\_name:password:GID:user\_list

* [Previous](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.4.5)
* [Next](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.5)

## 13.5 Who is On the System

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

* [Previous](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.4.6)
* [Next](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.5.1)

## 13.5.1 Step 1

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

who

**sysadmin@localhost:~$** who

sysadmin console Apr 11 14:32

**sysadmin@localhost:~$**

The output of the who command has four columns:

**Username**

sysadmin console Apr 11 14:32

This column indicates the name of the user who is logged in.

**Terminal**

sysadmin console Apr 11 14:32

This column indicates which terminal window the user is working in.

**Date**

sysadmin console Apr 11 14:32

This column indicates when the user logged in.

**Host**

Although there is no output for the fourth column in this case, it can be the name or IP address of a local or remote host.

* [Previous](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.5)
* [Next](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.5.2)

## 13.5.2 Step 2

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

w

**sysadmin@localhost:~$** w

13:17:08 up 6 days, 13 min, 1 user, load average: 0.39, 0.34, 0.37

USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT

sysadmin console 14:32 4.00s 0.16s 0.00s w

**sysadmin@localhost:~$**

Output from the w command displays a summary of how long the system has been running, how many users are logged in and the system load averages for the past 1, 5, and 13 minutes.

Also displayed is an entry for each user with their login name, tty name (terminal name), host, login time, idle time, JCPU (CPU time used by background jobs), PCPU (CPU time used by the current process) and what is executing on the current command line.

* [Previous](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.5.1)
* [Next](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.6)

## 13.6 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.

* [Previous](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.5.2)
* [Next](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.6.1)

## 13.6.1 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.

last

**sysadmin@localhost:~$** last

sysadmin console Tue Sep 18 02:31 still logged in

sysadmin console Tue Sep 18 02:31 - 02:31 (00:00)

wtmp begins Tue Sep 18 02:31:57 2018

* [Previous](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/15.6)
* [Next](https://content.netdevgroup.com/labs/linux-essentials/oTPPyuJYdJ/)