Linux List Users

At any time, more than one user can access an individual computer system. With these types of distributed systems, the system administrators should take accurate security measures so that a user can't break the other's privacy.

For example,

Using the access control mechanism, that defines the privileges of all the users.

A modification in the privileges of users may be mandatory. For example, the user may require her or his privileges grown for a specific task, or a capability of a specific user for accessing the system might have to be entirely revoked.

In these types of scenarios, it is essential for a system administrator for having enough knowledge of each user of a system.
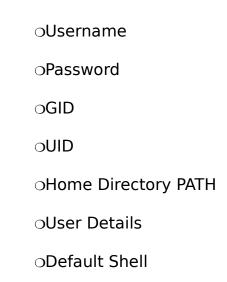
In this topic, we will explore the techniques used for **listing the users** of the Linux operating system. Both **command-line interface-**based techniques and the **graphical user interface-based techniques** could be used for this operation.

/etc/passwd File

The details of the users are stored inside the /etc/passwd file. This file is a plain text file. Hence, we can read this file using a cat or less command.

In this file, every line includes various details about that particular user isolated by a colon (:).

A single line has the following details isolated by a colon (:).

○Username

○Password

○GID

○UID

○Home Directory PATH

○User Details

○Default Shell

Username- It is a login name of a user. It cannot have spaces or other unique characters. There are alphanumeric characters are permitted only.

Password- The password is saved on the /etc/shadow file in a Linux-based operating system.

GID- All the groups have a numeric ID and a group name which is known as GID or Group ID on Linux-based operating systems. All the users on Linux should be a member of at least a single group.

Hence, for all the users created, the group is also created along with a similar name as the username. Then the user is added to the group. The group ID of the main group is added in this specific field. This main group is the group of the user (default).

When the user is a member of several groups, she/he can modify it while she/he is logged inside with the newgrp command. The GUD begins from 1000 for ordinary groups.

If our Linux is not configured specifically, the Group ID must be similar to the UID.

> Note: The root group contains the GID 0.

UID- All the users have a numeric ID and username, or an alphanumeric name which is known as UID or User ID. The UID begins from 1000 for ordinary users and the root user contains the UID 0.

Home Directory Path- It contains a path to the directory in which every user file would be saved. A shell variable that is $HOME is set through this field.

User Details- It contains the complete name and other details about the user as a comma isolated list. One of the most basic uses of this step is to set the user's full name. Just type inside the full name of our user name here and it must be set.

Default Shell- We should have a set of the shell for our users on Linux-based systems. By default, the **bash** and **sh (/bin/sh)** shell must be set for users who are capable of logging into the system. However, there are also other shells like csh, zsh, etc.

The users of the system have the **/sbin/nologin** shell set; hence, they would not be capable of logging into the system. If we wish to disable the login process for a few users, set this field for these types of users to /sbin/nologin.

Sort and list users by their name

We can sort and list the users in alphabetical order. For doing this, we would apply the previous command and also include the sort command.

The command would be as follows:

cut -d: -f1 /etc/passwd | sort

```
karishma@karishma-Vostro-3446:~$ cut -d: -f1 /etc/passwd | sort
_apt
avahi
avahi-autoipd
backup
bin
colord
cups-pk-helper
daemon
dnsmasq
games
gdm
geoclue
gnats
gnome-initial-setup
hplip
irc
karishma
kernoops
list
lp
mail
man
messagebus
news
nm-openvpn
nobody
nvidia-persistenced
proxy
pulse
root
rtkit
saned
speech-dispatcher
sssd
sync
sys
syslog
```

After using the above command the users are displayed sorted.

List the users with no password

It is necessary to know those users who haven't password and for taking the necessary action. For listing users who don't have any password, we can apply the below command:

sudo getent shadow | grep -Po '^[^:]*(?=:.?:)'

```
karishma@karishma-Vostro-3446:~$ sudo getent shadow | grep -Po '^[^:]*(?=:.?:)'
[sudo] password for karishma:
root
daemon
bin
sys
sync
games
man
lp
mail
news
uucp
proxy
www-data
backup
list
irc
gnats
nobody
systemd-timesync
systemd-network
systemd-resolve
messagebus
syslog
_apt
tss
uuidd
tcpdump
avahi-autoipd
usbmux
rtkit
dnsmasq
avahi
cups-pk-helper
speech-dispatcher
kernoops
saned
```

After using the above command, we will get the list of users without a password.

List the users through disk usage

We can apply the **du** command for getting the disk usage if we have a large directory and we wish to aware of which user is overflowing it.

Using this command, we can find which of the users are corrupting the disk space.

The command will be as follows:

1. $ sudo du -smc /home/* | sort -n

```
karishma@karishma-Vostro-3446:~$ sudo du -smc /home/* | sort -n
1028     /home/karishma
1028     total
karishma@karishma-Vostro-3446:~$ ▯
```

After using the above command, we will have the list of users ordered through the disk usage for the directory /home.

List the logged users (currently)

We have a lot of ways for listing the logged-in users (currently). In the first way we can apply the user command:

1. $ users

```
karishma@karishma-Vostro-3446:~$ users
karishma
karishma@karishma-Vostro-3446:~$ ▯
```

The above command will list the users along with open sessions inside the system.

However, this information is a bit common. But, we have other commands which provide more details. Simply, the command is w.

1. $ w

```
karishma@karishma-Vostro-3446:~$ w
 12:51:51 up 31 min,  1 user,  load average: 0.37, 0.35, 0.31
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
karishma :0       :0               12:22    ?xdm?  2:32   0.01s /usr/libexec/gdm
karishma@karishma-Vostro-3446:~$ ▯
```

We will get more details like the exact time in which the session was begun and the terminal session was available.

Now, there is another command known as **who**. This command exists to the whole family of UNIX. So, we can apply it to another system such as FreeBSD.

1. $ who

Using the above command, we have also some details about logged-in users currently. We can include the **-a** option and display every detail.

who -a

List the logged users (recently)

We examined how to get the logged-in users currently, but what about list out the user's login history?

We can apply the last command for getting more details of the logins:

1. $ last

```
karishma@karishma-Vostro-3446:~$ last
karishma :0           :0               Thu Apr 15 12:22    still logged in
reboot   system boot  5.8.0-41-generic Thu Apr 15 12:20    still running
karishma :0           :0               Thu Apr 15 12:18 - down   (00:00)
reboot   system boot  5.8.0-41-generic Thu Apr 15 12:17 - 12:19  (00:02)
karishma :0           :0               Wed Apr 14 23:43 - down   (02:09)
reboot   system boot  5.8.0-41-generic Wed Apr 14 23:42 - 01:53  (02:10)
karishma :0           :0               Wed Apr 14 19:16 - down   (02:56)
reboot   system boot  5.8.0-41-generic Wed Apr 14 19:15 - 22:13  (02:57)
karishma :0           :0               Wed Apr 14 18:06 - down   (00:15)
reboot   system boot  5.8.0-41-generic Wed Apr 14 18:04 - 18:21  (00:17)
karishma :0           :0               Tue Apr 13 16:27 - down   (00:02)
reboot   system boot  5.8.0-41-generic Tue Apr 13 16:25 - 16:30  (00:04)
karishma :0           :0               Tue Apr 13 16:09 - crash  (00:16)
reboot   system boot  5.8.0-41-generic Tue Apr 13 16:08 - 16:30  (00:21)
karishma :0           :0               Sun Apr 11 18:09 - down   (00:18)
reboot   system boot  5.8.0-41-generic Sun Apr 11 18:07 - 18:27  (00:19)
karishma :0           :0               Sat Apr 10 20:36 - down   (00:14)
reboot   system boot  5.8.0-41-generic Sat Apr 10 20:35 - 20:51  (00:15)
karishma :0           :0               Fri Apr  9 22:13 - down   (00:20)
reboot   system boot  5.8.0-41-generic Fri Apr  9 22:12 - 22:33  (00:21)
karishma :0           :0               Fri Apr  9 17:44 - down   (00:53)
reboot   system boot  5.8.0-41-generic Fri Apr  9 17:43 - 18:38  (00:54)
karishma :0           :0               Thu Apr  8 20:13 - down   (00:18)
reboot   system boot  5.8.0-41-generic Thu Apr  8 20:12 - 20:32  (00:19)
karishma :0           :0               Thu Apr  8 17:23 - down   (00:12)
reboot   system boot  5.8.0-41-generic Thu Apr  8 17:22 - 17:36  (00:14)
karishma :0           :0               Thu Apr  8 14:08 - down   (00:04)
reboot   system boot  5.8.0-41-generic Thu Apr  8 14:06 - 14:12  (00:05)
karishma :0           :0               Wed Apr  7 16:38 - down   (00:53)
reboot   system boot  5.8.0-41-generic Wed Apr  7 16:36 - 17:31  (00:54)
karishma :0           :0               Tue Apr  6 17:34 - down   (00:20)
reboot   system boot  5.8.0-41-generic Tue Apr  6 17:32 - 17:54  (00:22)
karishma :0           :0               Mon Apr  5 17:35 - down   (00:14)
reboot   system boot  5.8.0-41-generic Mon Apr  5 17:33 - 17:49  (00:15)
karishma :0           :0               Sun Apr  4 11:23 - down   (00:32)
reboot   system boot  5.8.0-41-generic Sun Apr  4 11:21 - 11:56  (00:34)
karishma :0           :0               Sat Apr  3 17:22 - down   (00:11)
```

Also, we can get the logins of a specific user by using the following command:

1. $ last [username]

All we have to do is select an exact time and date for listing who logged at that specific time.

List the root users

Usually, there is only a single root user in Linux operating system. When there are several then how to list them?

For doing this, we can apply the following command:

 grep 'x:0:' /etc/passwd

```
karishma@karishma-Vostro-3446:~$ grep 'x:0:' /etc/passwd
root:x:0:0:root:/root:/bin/bash
karishma@karishma-Vostro-3446:~$ ▯
```

We can filter the file for getting users along with zero UID root users by using the above command.

Another method by inspecting the /etc/group file:

grep root /etc/group

```
karishma@karishma-Vostro-3446:~$ grep root /etc/group
root:x:0:
karishma@karishma-Vostro-3446:~$ ▯
```

Here we will get the users inside the group route through the /etc/passwd file.

We can also check when any user can run commands as the root by inspecting the file:

1. $ cat /etc/sudoers

List every user of a group

In Linux, there are two important ways for listing the users of a group. The most direct and easiest way for getting the members through the **/etc/group** files like below:

1. $ cat /etc/group | grep group1
   The above command will list members inside the group1 group.

The second way is by applying commands such as the member's command inside the Debian-based distros. By default, it is not installed in Linux distributions.

List the number of users

In Linux, to list the number of users, we can count lines inside the **/etc/passwd** file with the help of the **wc** command which is as follows:

cut -d: -f1 /etc/passwd | wc -l

The above command will provide us the regular and system users.

Get sudo users

Linux systems include a utility known as sudo that permits us to run commands as when we were another user usually who is a root user.

It must be managed with care inside the professional environment.

It is also very essential for knowing which user can execute the sudo command. It is sufficient for listing the users that are related to the sudo group.

1. $ members sudo

Users inside this group can run the commands as the super users.

List the users with SSH access

SSH permits users for accessing remote computers on the network. This method is secure and was developed as a substitute for Telnet.

Every regular user can by default login and access SSH. If we wish to restrict it, we can apply the configuration file of SSH (/etc/ssh/ssh_config) and include the directive below:

1. AllowUsers user1 user2 user3
   We can also permit groups rather than permitting users only applying the AllowGroups directive:

1. AllowGroups group1 group2 group3
   These types of directives specify who can use the service. We should not forget to reboot the SSH service.

List the users who have access to a directory or file

We can provide multiple user permissions to modify or access the directories and files in two methods.

In the first method, we can add the users to a group of the directory or file.

We can get the group members with the help of member utility.

But, what when we wish this user for having access to this particular file only (not each group permission)?

For this, we can use the ACL for this particular file with the help of the setfacl command like below:

1. $ setfacl -m u:newuser:rwx test
   Here, we provide the user known as the **newuser** the authentication for the file known as **test**. It act as a authentications of reading, write, and execution.

   Now, the file could be modified or accessed by the owner. The user is known as a **newuser**. Hence, how to list them?

   With the help of the getfacl command, we can get them:

1. $ getfacl test
   We can get every user using the above command who has authentications for the file along with their related permissions.

List the disabled (locked) users

We could lock any user as the security measures in Linux operating system. It is a precaution when it is uncertain that the user is implementing things wrong, and we do not wish to remove the user completely and only lock them for investigation.

We can apply the following command to lock the user:

1. $ usermod -L user1

```
karishma@karishma-Vostro-3446:~$ usermod -L user1
usermod: user 'user1' does not exist
karishma@karishma-Vostro-3446:~$ []
```

After applying the above command, the user named user1' will no longer be capable to use or login into the system.

List the remote users (LDAP)

We can list remote and local users using a single command known as **getent.**

getent passwd

```
karishma@karishma-Vostro-3446:~/mydir$ getent 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:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:101:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:114::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:115::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:109:117:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:110:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
rtkit:x:111:118:RealtimeKit,,,:/proc:/usr/sbin/nologin
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
avahi:x:113:120:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
cups-pk-helper:x:114:121:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
speech-dispatcher:x:115:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/usr/sbin/nologin
saned:x:117:123::/var/lib/saned:/usr/sbin/nologin
nm-openvpn:x:118:124:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
```

The above command will list both NIS or NDAP users and local system users or other network users.

We can pipe the outcomes of this command to the above-mentioned commands in a similar way.

The getent command can also list the accounts of a group like below:

getent group

```
karishma@karishma-Vostro-3446:~/mydir$ getent group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,karishma
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:karishma
floppy:x:25:
tape:x:26:
sudo:x:27:karishma
audio:x:29:pulse
dip:x:30:karishma
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
gnats:x:41:
shadow:x:42:
utmp:x:43:
video:x:44:
sasl:x:45:
plugdev:x:46:karishma
staff:x:50:
games:x:60:
```

We can inspect the command's man page to understand the other databases that the command could find in.

Techniques to List the Users

Technique 1: The "cat" command

We can list each user on the command line to show each user's password and account details in the file /etc/passwd of Linux using the cat command.

To apply the cat command for listing each user in Linux operating system, The below steps must be implemented in sequence:

o Launch the terminal.

o Execute the below command.

cat /etc/passwd

```
karishma@karishma-Vostro-3446:~$ cat /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
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:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:101:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:114::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:115::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:109:117:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:110:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
rtkit:x:111:118:RealtimeKit,,,:/proc:/usr/sbin/nologin
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
avahi:x:113:120:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
cups-pk-helper:x:114:121:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
speech-dispatcher:x:115:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/usr/sbin/nologin
saned:x:117:123::/var/lib/saned:/usr/sbin/nologin
nm-openvpn:x:118:124:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
```

Running the command will show the usernames and some other information as well. We can scroll this list for viewing each user of the Linux operating system.

Technique 2: The "awk" command

This command is useful if we want to show only user names which may be helpful if we don't require any technical information to be returned using the cat command

To apply this command for listing every user in Linux, the below steps must be implemented in sequence.

○Launch the terminal.

○Execute the below command:

awk-F: '{ print $1}' /etc/passwd

When we execute this command in our terminal, we will receive user names only. Also, this list contains every user of our Linux system.

Technique 3: The "compgen" command

The compgen command is applied to show user names only and it is avoiding every other information.

T

o apply the compgen command for listing every user of Linux, the below steps must be implemented in sequence:

○Launch the terminal.

○Execute the below command:

compgen -u

```
karishma@karishma-Vostro-3446:~$ compgen -u
root
daemon
bin
sys
sync
games
man
lp
mail
news
uucp
proxy
www-data
backup
list
irc
gnats
nobody
systemd-timesync
systemd-network
systemd-resolve
messagebus
syslog
_apt
tss
uuidd
tcpdump
avahi-autoipd
usbmux
rtkit
dnsmasq
avahi
cups-pk-helper
speech-dispatcher
kernoops
saned
nm-openvpn
```

We will get every user name connected with our Linux operating system using this command.

Technique 4: The "getent" command

The result of the cat command is very similar to that of the getent command because it shows several details with the usernames.

To apply the getent command for listing every user inside Linux, the below steps must be implemented in sequence:

- Launch the terminal.

○Execute the below command:

1. $ getent passwd

```
karishma@karishma-Vostro-3446:~$ getent 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:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:101:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:114::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:115::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:109:117:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:110:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
rtkit:x:111:118:RealtimeKit,,,:/proc:/usr/sbin/nologin
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
avahi:x:113:120:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
cups-pk-helper:x:114:121:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
speech-dispatcher:x:115:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/usr/sbin/nologin
saned:x:117:123::/var/lib/saned:/usr/sbin/nologin
nm-openvpn:x:118:124:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
```

The above command will list every user of our Linux system and some other information as well.