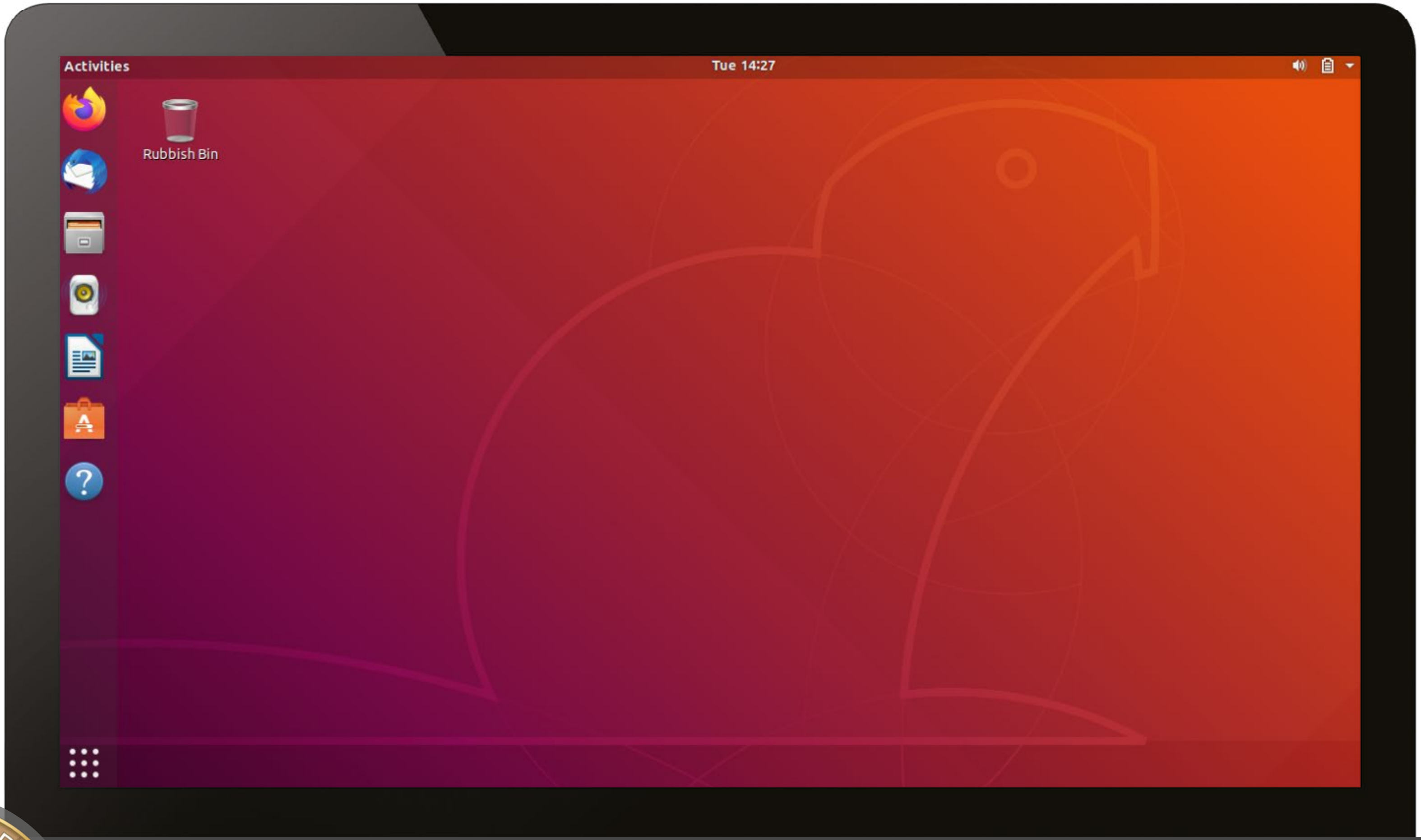


Ubuntu Advanced Cyber Security

Contents

ubuntu

As part of this guide, you will:

- demonstrate how to display groups, add, and remove groups and add/remove a user to a group
- demonstrate how to enable and disable automatic login
- define what the root account is and how to disable the root account
- identify the permissions that can be set on files/folders and how to edit these permissions
- define what the SSH is and how to enable and disable the SSH
- define the purpose of auditing and how to install and use Lynis as an auditing tool
- demonstrate how to install and use Webmin

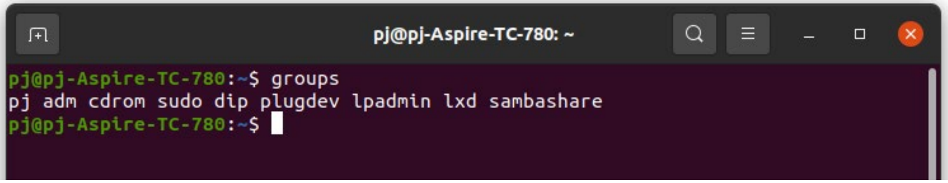
Groups

The purpose of groups is to allow permissions to be set across files and folders in a simpler way than going into each user and setting the permissions individually.

Displaying groups

To find out what groups a user is part of they would need to use the command:

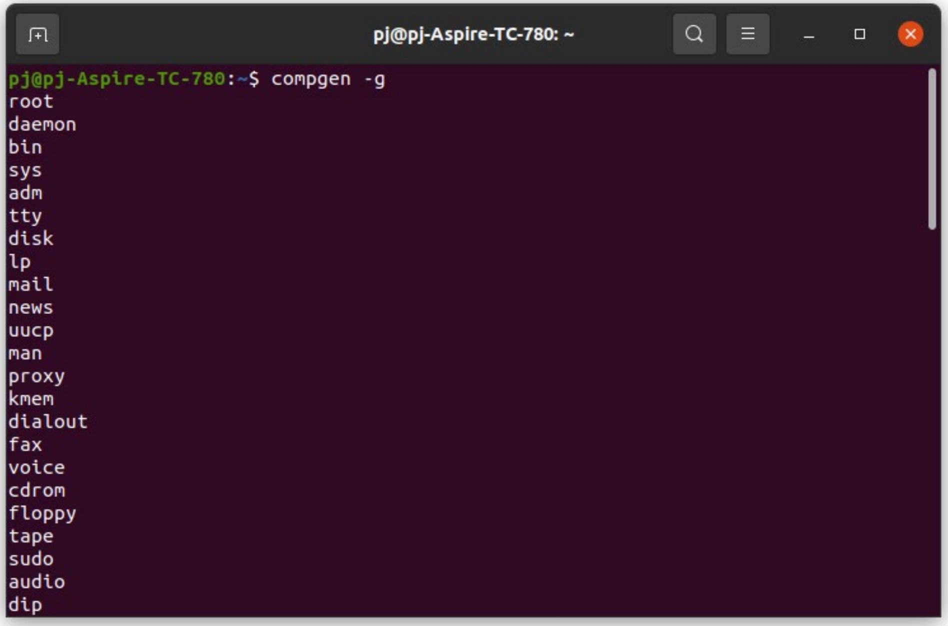
```
groups
```



```
pj@pj-Aspire-TC-780:~$ groups
pj adm cdrom sudo dip plugdev lpadmin lxd sambashare
pj@pj-Aspire-TC-780:~$
```

To view all groups that are set up on Ubuntu use the command:

```
compgen -g
```



```
pj@pj-Aspire-TC-780:~$ compgen -g
root
daemon
bin
sys
adm
tty
disk
lp
mail
news
uucp
man
proxy
kmem
dialout
fax
voice
cdrom
floppy
tape
sudo
audio
dip
```

To view all the groups with the group name, password, ID, and users, you use the command:

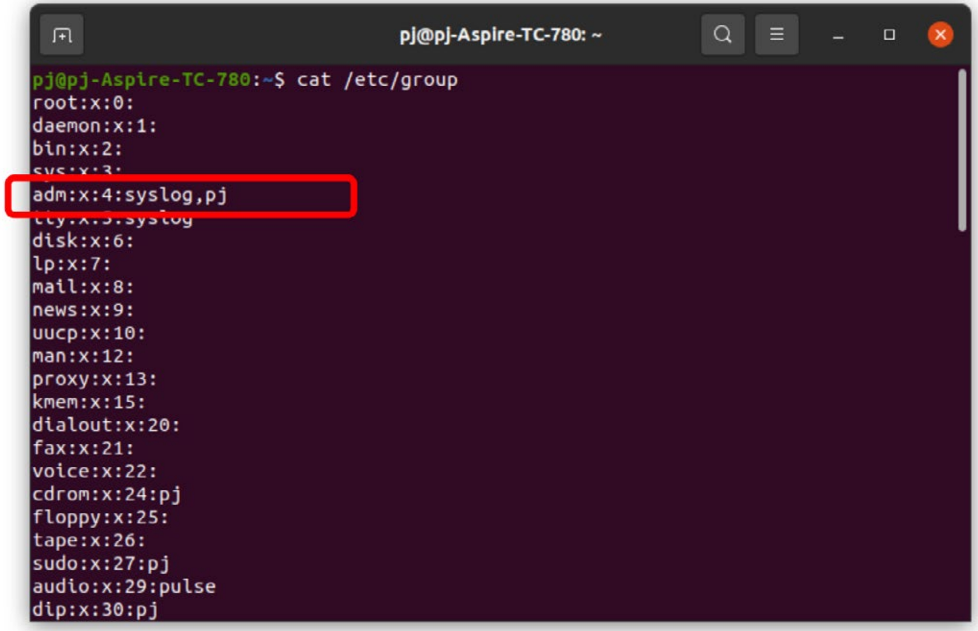
`cat /etc/group`

This file will display the group name, the password, group ID and list of users

If you look at the group **adm**, let's look at what the row tells us about the group.

`adm:x:4:syslog,pj`

- The group name is **adm**
- The password is labelled as **x**
- The group ID is **4**
- The users are **syslog** and **pj**



```
pj@pj-Aspire-TC-780:~$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,pj
tty:x:5:syslog
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:pj
floppy:x:25:
tape:x:26:
sudo:x:27:pj
audio:x:29:pulse
dip:x:30:pj
```

For security reasons the placeholder **x** is placed where the password should be, and this has been moved to another file.

You will notice that the first returned group is called **root**, every system will have this group and it will always hold position 0.

To view the users who have access to a group use the command:

```
getent group adm
```

Replace **adm** with the group name you are looking at.

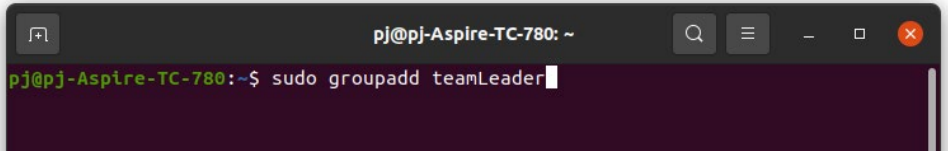
Adding a group

To add a group, you use the command **groupadd** and in this instance use the admin level command too.

```
sudo groupadd teamLeader
```

The group name is inserted after the command groupadd and can be any name you want (without spaces).

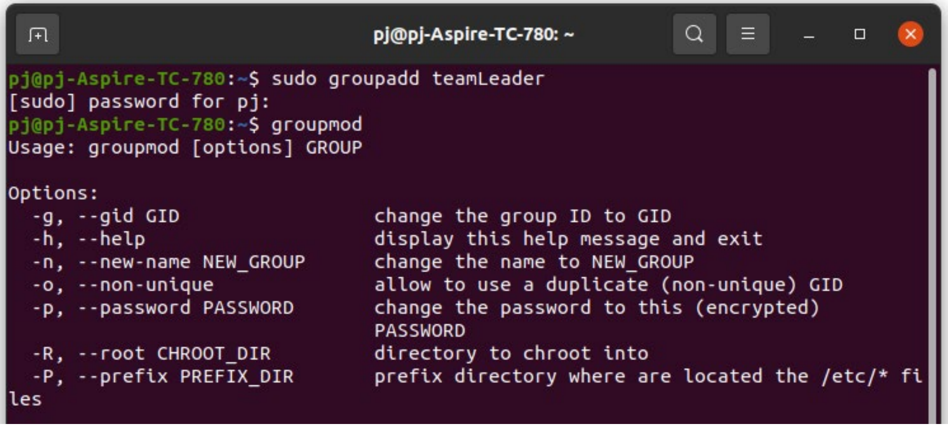
The same as every time you use the **sudo** command, you will be required to enter your password to complete the required steps.



```
pj@pj-Aspire-TC-780:~$ sudo groupadd teamLeader
```

If you now use the command **groupmod** you will be able to view and edit the specifics around the group set up.

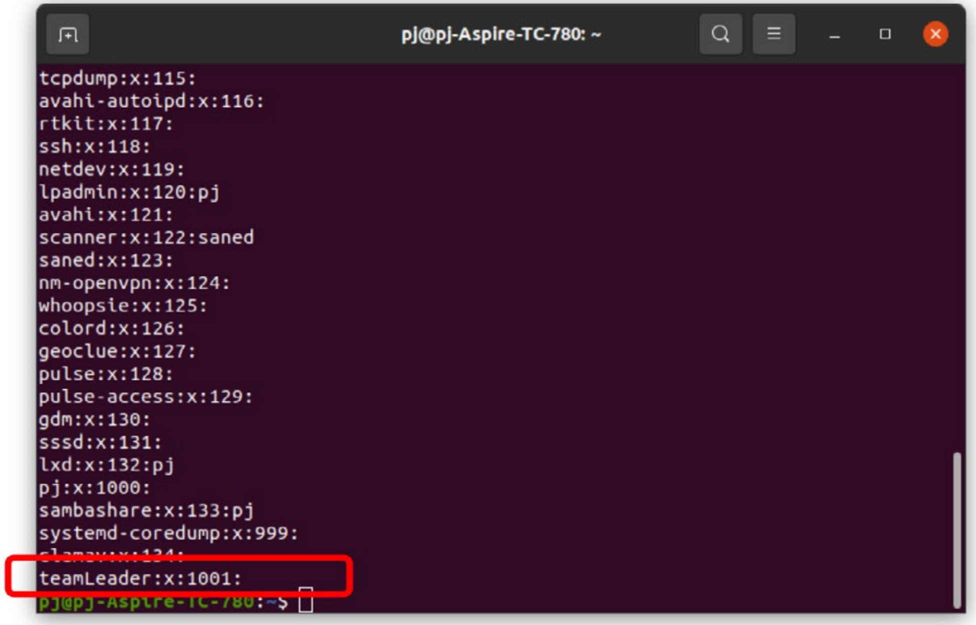
```
groupmod
```



```
pj@pj-Aspire-TC-780:~$ sudo groupadd teamLeader
[sudo] password for pj:
pj@pj-Aspire-TC-780:~$ groupmod
Usage: groupmod [options] GROUP

Options:
  -g, --gid GID                 change the group ID to GID
  -h, --help                    display this help message and exit
  -n, --new-name NEW_GROUP      change the name to NEW_GROUP
  -o, --non-unique              allow to use a duplicate (non-unique) GID
  -p, --password PASSWORD       change the password to this (encrypted)
                                PASSWORD
  -R, --root CHROOT_DIR         directory to chroot into
  -P, --prefix PREFIX_DIR       prefix directory where are located the /etc/* fi
les
```

Cyber-Security Fact:
Changing any settings should be considered fully to ensure you are changing the correct settings and for the correct reasons. Settings are there to protect the system from users making mistakes and/or editing systems further.

If you now use the command `cat /etc/group` or `compgen -g` you will see the group now added to the list of groups in the list.



```
tcpdump:x:115:
avahi-autoipd:x:116:
rtkit:x:117:
ssh:x:118:
netdev:x:119:
lpadmin:x:120:pj
avahi:x:121:
scanner:x:122:saned
saned:x:123:
nm-openvpn:x:124:
whoopsie:x:125:
colord:x:126:
geoclue:x:127:
pulse:x:128:
pulse-access:x:129:
gdm:x:130:
sssd:x:131:
lxd:x:132:pj
pj:x:1000:
sambashare:x:133:pj
systemd-coredump:x:999:
clamav:x:134:
teamLeader:x:1001:
pj@pj-Aspire-TC-780:~$ 
```

We can see the set up for the group now as:

- The group name is **teamLeader**
- The password is labelled as **x**
- The group ID is **1001**
- There are no users in the group yet

Adding a user to/from a group

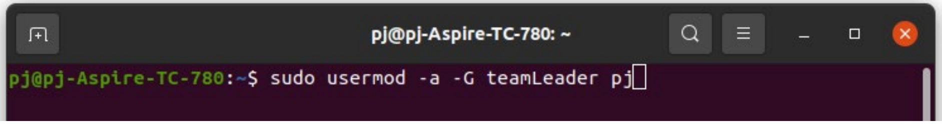
To add a user to the group we need to use the command

`usermod`

To add a user to the group you use the command line:

`sudo useradd -a -G teamLeader pj`

`teamLeader` *is the name of the group and after the group you add the username.*

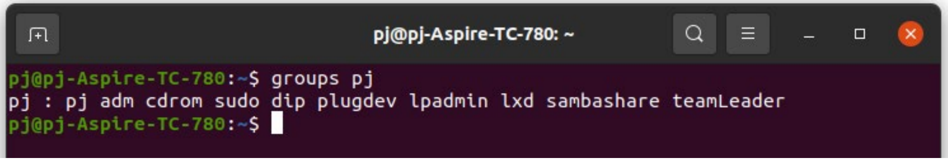


```
pj@pj-Aspire-TC-780:~$ sudo usermod -a -G teamLeader pj
```

The same as every time you use the **sudo** command, you will be required to enter your password to complete the required steps.

To view the user **`pj`** and the groups they are assigned to, as well as check if the group **`teamLeader`** has been added, use the command line:

`groups pj`

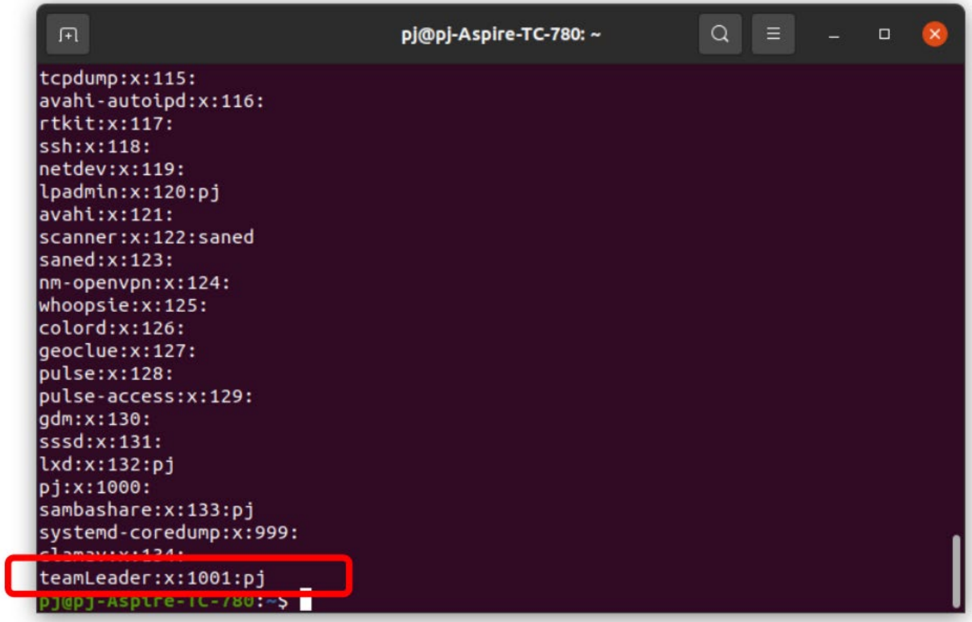


```
pj@pj-Aspire-TC-780:~$ groups pj
pj : pj adm cdrom sudo dip plugdev lpadmin lxd sambashare teamLeader
pj@pj-Aspire-TC-780:~$ 
```

Let's also check the set up of the group and the user assigned using the command:

`cat /etc/group`

You can see that at the bottom of the list of groups we have the group added **`teamLeader`**, but we now have the user **`pj`** added after the group ID.



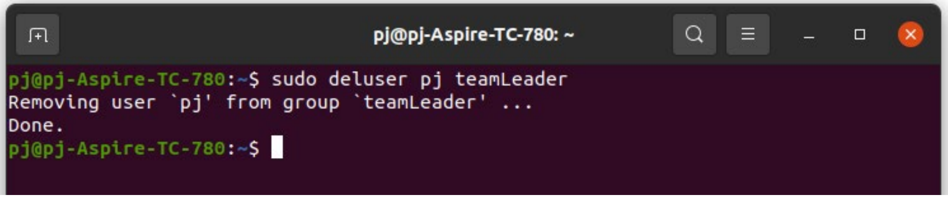
```
tcpdump:x:115:
avahi-autoipd:x:116:
rtkit:x:117:
ssh:x:118:
netdev:x:119:
lpadmin:x:120:pj
avahi:x:121:
scanner:x:122:saned
saned:x:123:
nm-openvpn:x:124:
whoopsie:x:125:
colord:x:126:
geoclue:x:127:
pulse:x:128:
pulse-access:x:129:
gdm:x:130:
sssd:x:131:
lxd:x:132:pj
pj:x:1000:
sambashare:x:133:pj
systemd-coredump:x:999:
clamav:x:134:
teamLeader:x:1001:pj
pj@pj-Aspire-TC-780:~$ 
```

Removing a user from a group

To remove a user from the group you need to use the command:

```
sudo deluser pj teamLeader
```

`deluser` is the command for deleting a user, you follow this with the user to remove and then the group that the user needs to be removed from.



```
pj@pj-Aspire-TC-780:~$ sudo deluser pj teamLeader
Removing user `pj' from group `teamLeader' ...
Done.
pj@pj-Aspire-TC-780:~$
```

You can check this has worked by using the command line again to see that the user is no longer associated with the group.

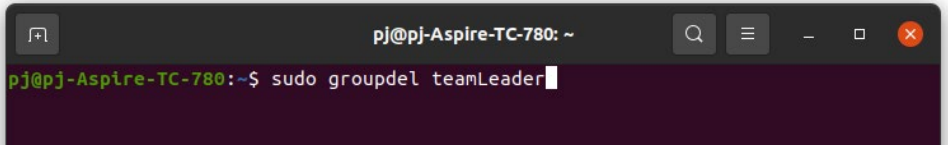
```
cat /etc/group
```

Removing a group

To remove a group altogether you need to use the command:

```
sudo groupdel teamLeader
```

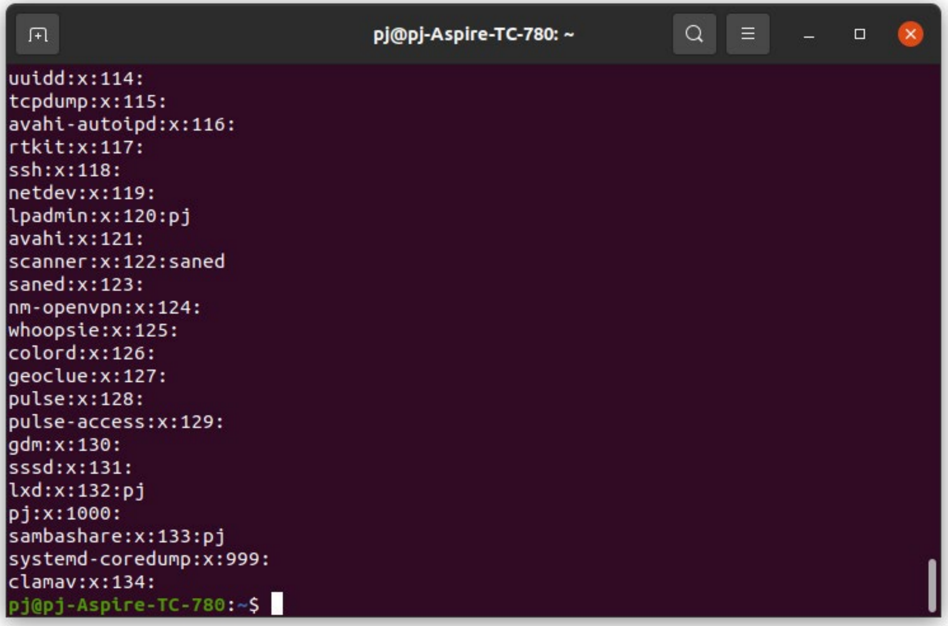
Replace **`teamLeader`** *with the group name you want to remove.*



```
pj@pj-Aspire-TC-780:~$ sudo groupdel teamLeader
```

It is slightly different this time as you do not get a response when you use this command to say that the group has been deleted. Best practice would be to check it has been removed from the list of groups in the same way as you have in other steps using the command:

```
cat /etc/group
```



```
uuidd:x:114:
tcpdump:x:115:
avahi-autoipd:x:116:
rtkit:x:117:
ssh:x:118:
netdev:x:119:
lpadmin:x:120:pj
avahi:x:121:
scanner:x:122:saned
saned:x:123:
nm-openvpn:x:124:
whoopsie:x:125:
colord:x:126:
geoclue:x:127:
pulse:x:128:
pulse-access:x:129:
gdm:x:130:
sssd:x:131:
lxd:x:132:pj
pj:x:1000:
sambashare:x:133:pj
systemd-coredump:x:999:
clamav:x:134:
pj@pj-Aspire-TC-780:~$
```

I can see from the response that the last group where it was listed previously has now changed and the group teamLeader has been removed.

Cyber-Security Fact:
Remember when adding and removing users from groups and creating groups to do so correctly as you are changing the settings on the system. User permissions using the sudo command should be used correctly and not delete/edit system groups without understanding fully.

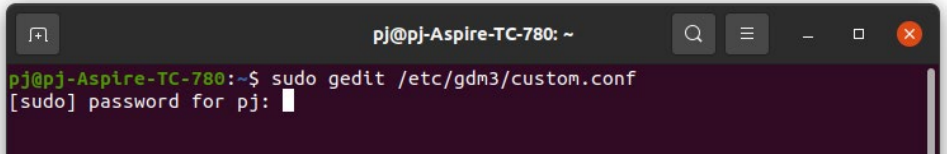
Automatic login

There are two ways to look at the automatic login settings. By default they are set as disabled for a user so that a password is required to enter the system.

Option 1 – Terminal

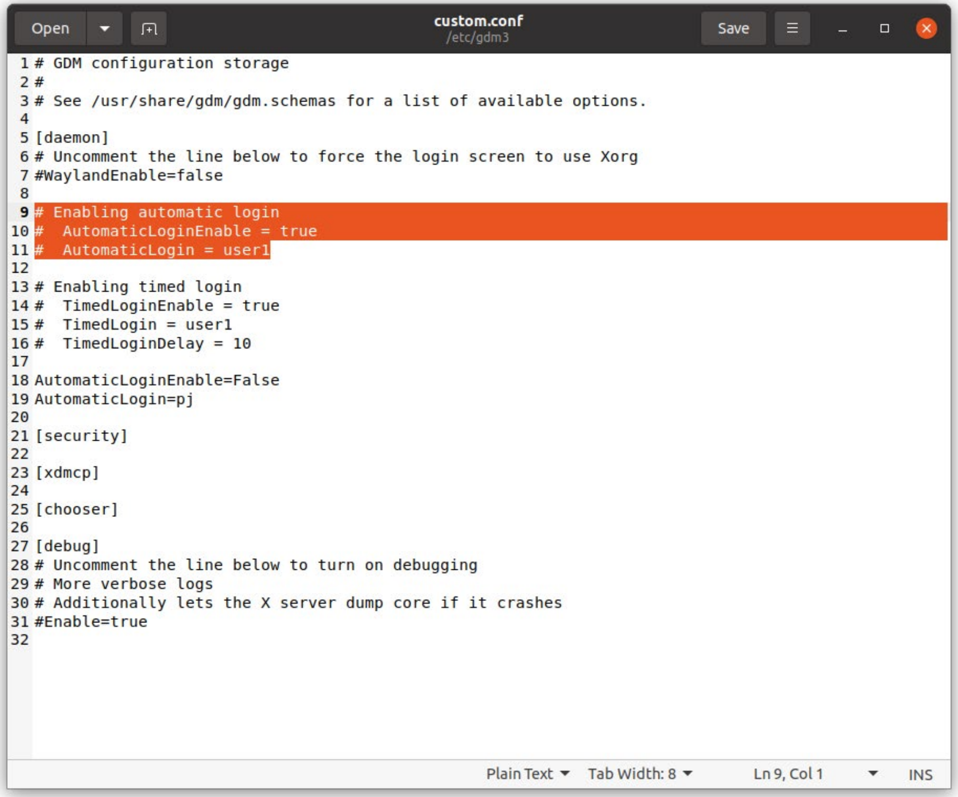
To open the file containing the configured settings you need to use the command:

```
sudo gedit /etc/gdm3/custom.conf
```



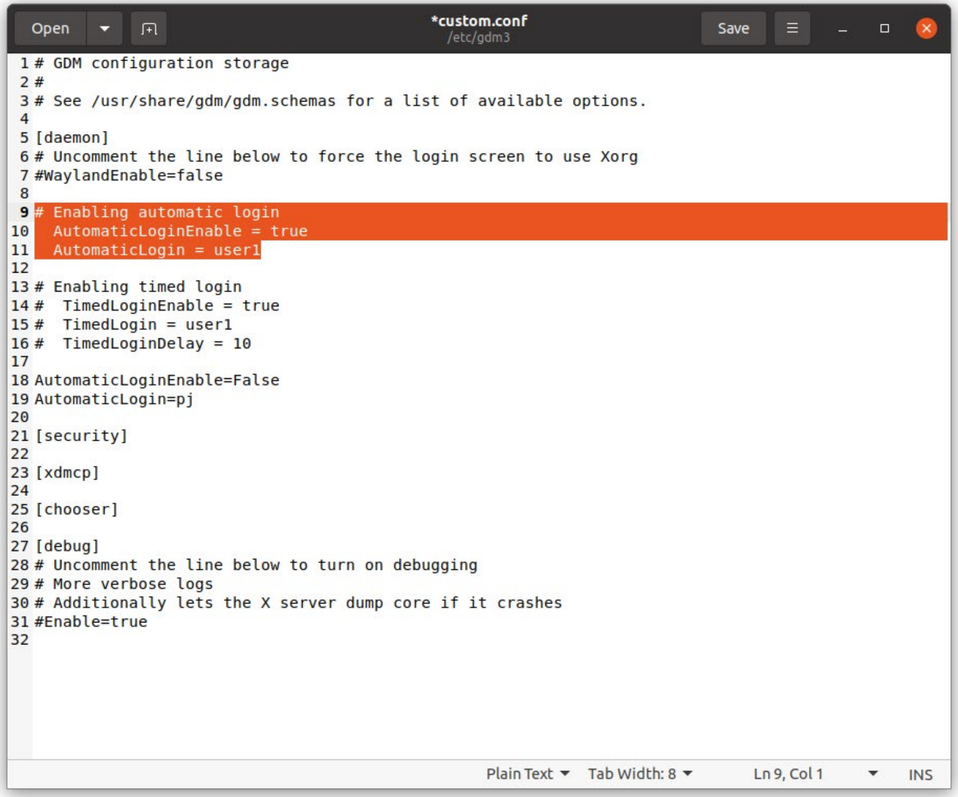
```
pj@pj-Aspire-TC-780:~$ sudo gedit /etc/gdm3/custom.conf
[sudo] password for pj:
```

After you have entered your password, you will see the file open and, in this file, we are looking at lines 9, 10 and 11.



```
 1 # GDM configuration storage
 2 #
 3 # See /usr/share/gdm/gdm.schemas for a list of available options.
 4
 5 [daemon]
 6 # Uncomment the line below to force the login screen to use Xorg
 7 #WaylandEnable=false
 8
 9 # Enabling automatic login
10 #  AutomaticLoginEnable = true
11 #  AutomaticLogin = user1
12
13 # Enabling timed login
14 #  TimedLoginEnable = true
15 #  TimedLogin = user1
16 #  TimedLoginDelay = 10
17
18 AutomaticLoginEnable=False
19 AutomaticLogin=pj
20
21 [security]
22
23 [xdmcp]
24
25 [chooser]
26
27 [debug]
28 # Uncomment the line below to turn on debugging
29 # More verbose logs
30 # Additionally lets the X server dump core if it crashes
31 #Enable=true
32
```

The # hastag at the start of the rows represents a comment in the code. This is ignored by the system when looking at the file. To enable the automatic login for the system you need to remove the hashtag # from rows 10 and 11.



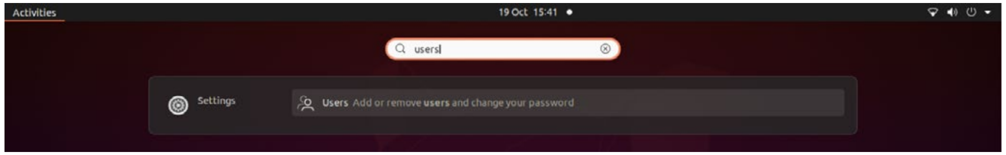
```
 1 # GDM configuration storage
 2 #
 3 # See /usr/share/gdm/gdm.schemas for a list of available options.
 4
 5 [daemon]
 6 # Uncomment the line below to force the login screen to use Xorg
 7 #WaylandEnable=false
 8
 9 # Enabling automatic login
10   AutomaticLoginEnable = true
11   AutomaticLogin = user1
12
13 # Enabling timed login
14 #  TimedLoginEnable = true
15 #  TimedLogin = user1
16 #  TimedLoginDelay = 10
17
18 AutomaticLoginEnable=False
19 AutomaticLogin=pj
20
21 [security]
22
23 [xdmcp]
24
25 [chooser]
26
27 [debug]
28 # Uncomment the line below to turn on debugging
29 # More verbose logs
30 # Additionally lets the X server dump core if it crashes
31 #Enable=true
32
```

Once you have completed this you need to select the save button on the top right of the open file.

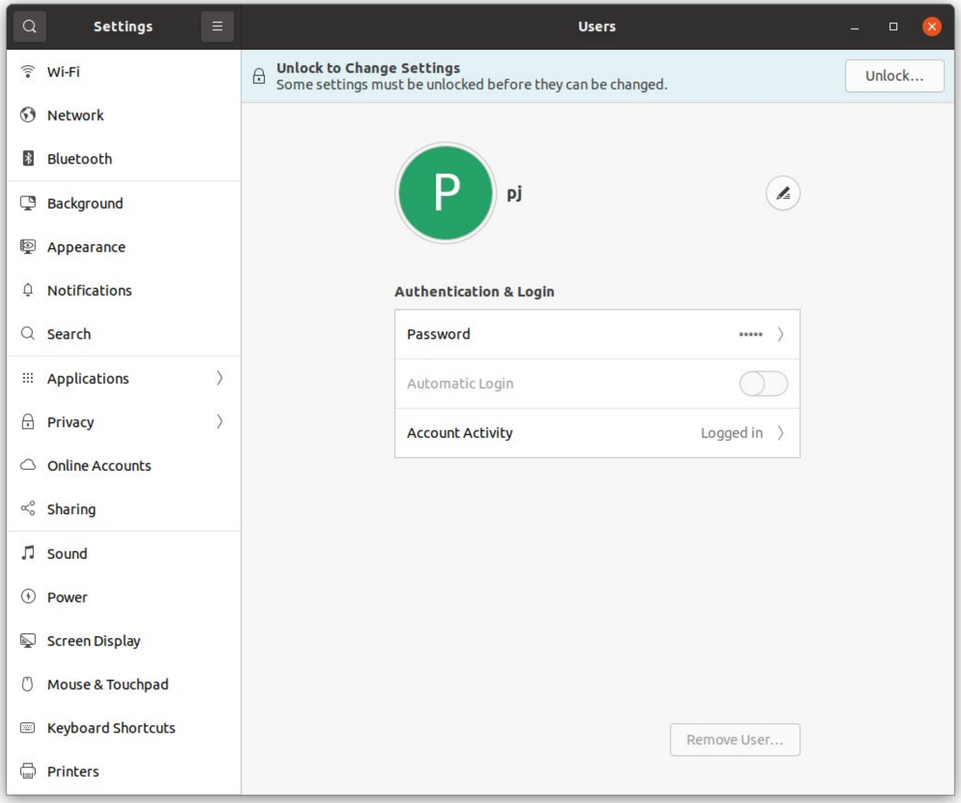
To **`disable`** automatic login, you would need to add the hashtag # back in to show that the lines of code are comments again and not actionable.

Option 2 – Users

If you click on **`Activities`** in the top left of the screen and then in the search box, type **`users`**. You will see the settings area to select.



When you open the settings area, you will be given the login information for the user. You will need to unlock to change settings by clicking unlock and when prompted, adding your password.

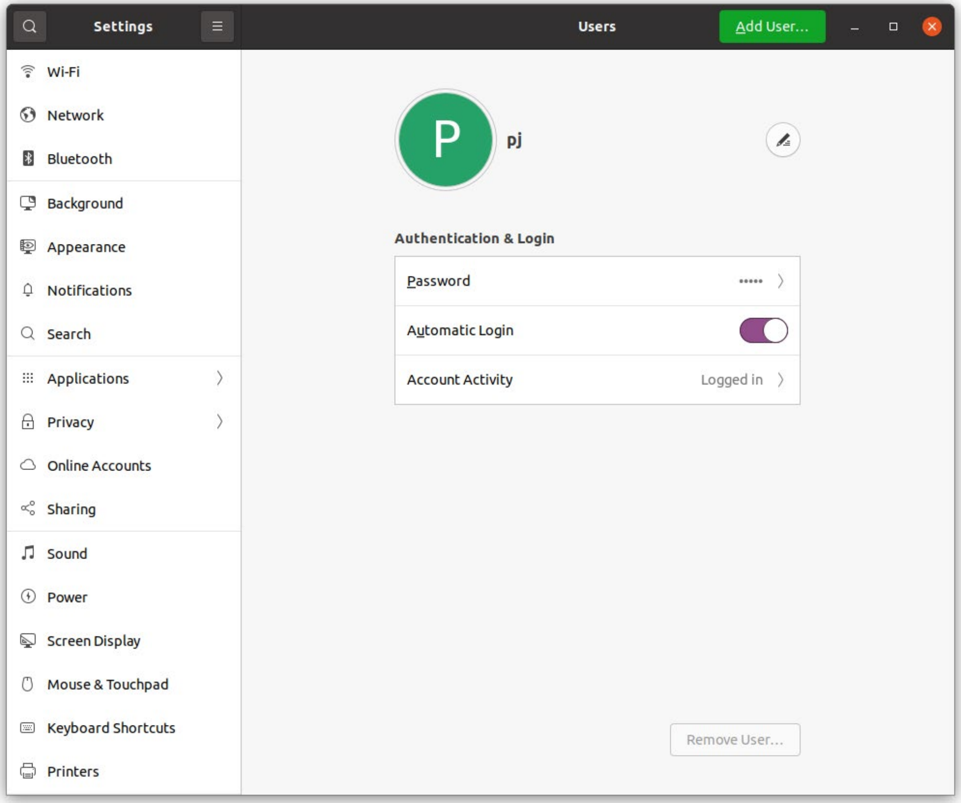


Unlock to Change Settings
Some settings must be unlocked before they can be changed.

Authentication & Login

Password	•••••
Automatic Login	○
Account Activity	Logged in

You will then be able to move the toggle to on to allow automatic login to enabled for this user.



Authentication & Login

Password	•••••
Automatic Login	●
Account Activity	Logged in

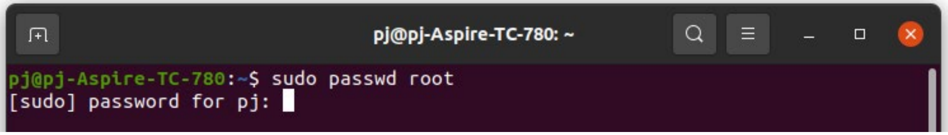
To disable the automatic login, you would move the toggle to `off`.

Default root account

On ubuntu there is a root account that is used and has permission to edit/add/delete any files or folders on the system. You have already learnt about using sudo and how this gives you access to administrative level permissions to perform some actions.

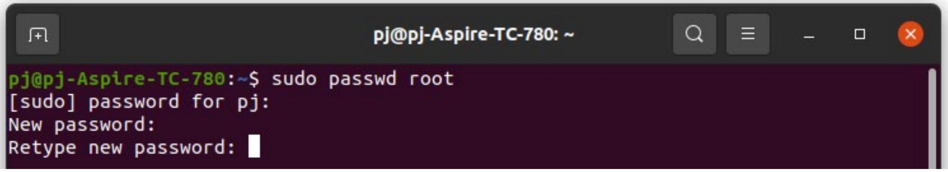
To enable the root account, you need to set a password for the root user and use the command:

```
sudo passwd root
```



```
pj@pj-Aspire-TC-780:~$ sudo passwd root
[sudo] password for pj: 
```

After you have entered your password for using sudo, you will be prompted to add a new password and then to retype the password. You will not see anything as you type.

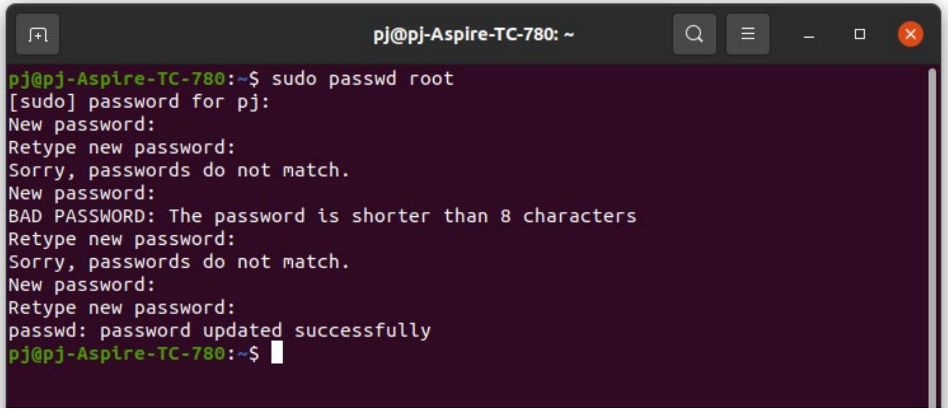


```
pj@pj-Aspire-TC-780:~$ sudo passwd root
[sudo] password for pj:
New password:
Retype new password: 
```

As you cannot see what is being typed, you may make a mistake and it is flagged up by telling you that the passwords do not match.

The password must also be a strong one and there is a mechanism for testing this and letting you know if the password you entered is a bad one.

Once you have added a strong password twice the password has been set and it will display that this has been set up successfully.



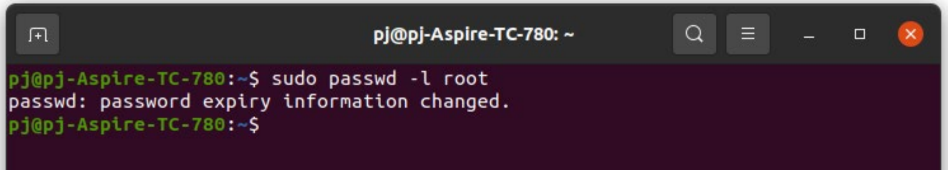
```
pj@pj-Aspire-TC-780:~$ sudo passwd root
[sudo] password for pj:
New password:
Retype new password:
Sorry, passwords do not match.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
Sorry, passwords do not match.
New password:
Retype new password:
passwd: password updated successfully
pj@pj-Aspire-TC-780:~$ 
```

Cyber-Security Fact:
It is imperative that the password set for the root account is a strong one as this user account will be able to change, add, delete anything on the system. Remember, a strong password is a mixture of upper and lowercase letters, numbers, and symbols, as well as over 8 characters long. The password should also be something that can not be guessed easily.

Cyber-Security Fact:
Make sure you think...once you are logged in as a root user you can delete everything on the system as well as potentially damage any files and folders. Unlike Windows where any major change is prompted by a 'are you sure' type message, there is none in Ubuntu, once you use a command it is final.

To disable the root account password, you need to set the password to expire using the command:

```
sudo passwd -l root
```

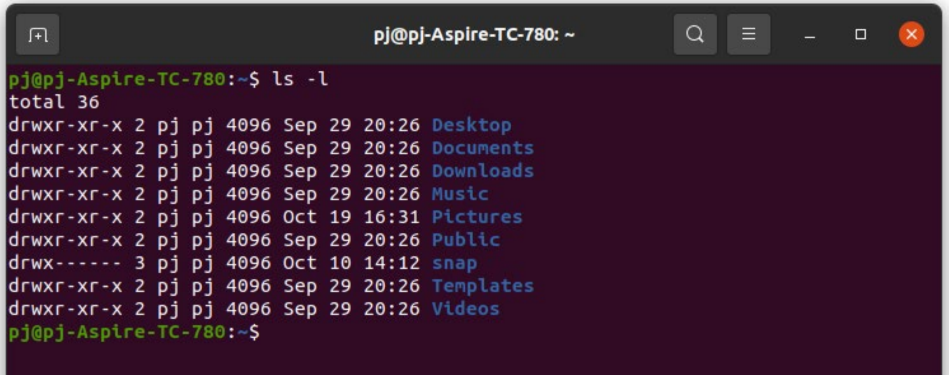


```
pj@pj-Aspire-TC-780:~$ sudo passwd -l root
passwd: password expiry information changed.
pj@pj-Aspire-TC-780:~$
```

Permissions

The permissions are set up on folders and files and you can view the files and folders set up on the computer using the command:

```
ls -l
```



```
pj@pj-Aspire-TC-780:~$ ls -l
total 36
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Desktop
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Documents
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Downloads
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Music
drwxr-xr-x 2 pj pj 4096 Oct 19 16:31 Pictures
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Public
drwx------ 3 pj pj 4096 Oct 10 14:12 snap
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Templates
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Videos
pj@pj-Aspire-TC-780:~$
```

You can see here that the folders that are set up are the main folders such as documents, pictures etc. On the left of each row, you can see a series of letters, and these represent the permissions set up on the folder/file.

d

`d` represents a directory

`-` represents a file

`l` represents a link

rwx

Read, Write, eXecute

For the owner of the file

r-x

Read - eXecute

For members of the group owning the file

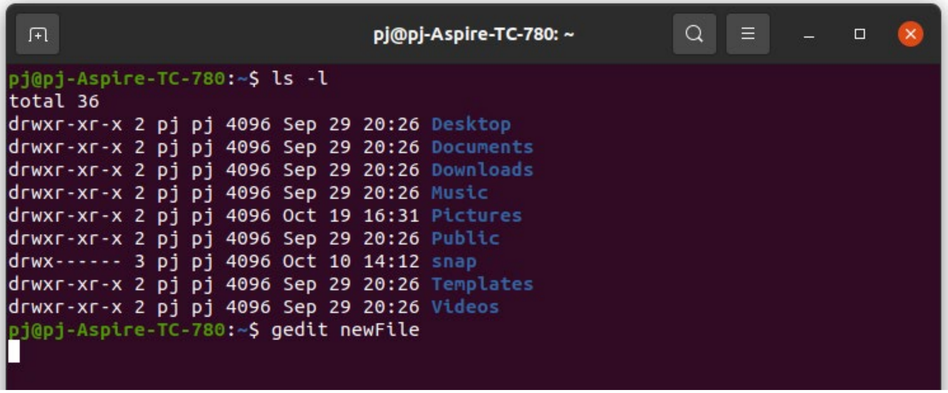
r-x

Read - eXecute

For other users

Let's create a new file called newFile use the following command:

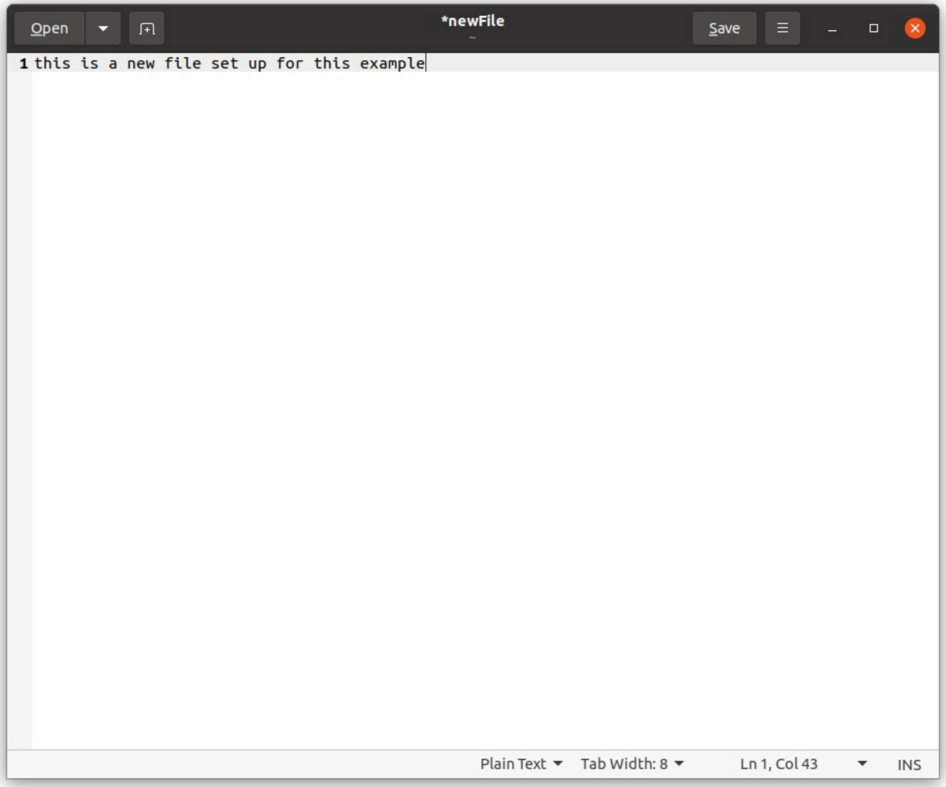
```
gedit newFile
```



```
pj@pj-Aspire-TC-780:~$ ls -l
total 36
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Desktop
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Documents
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Downloads
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Music
drwxr-xr-x 2 pj pj 4096 Oct 19 16:31 Pictures
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Public
drwx------ 3 pj pj 4096 Oct 10 14:12 snap
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Templates
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Videos
pj@pj-Aspire-TC-780:~$ gedit newFile
```

This will open the file in the text editor where you can create your file and save it. I have added some text and saved the file.

This will open the file in the text editor where you can create your file and save it. I have added some text and saved the file.

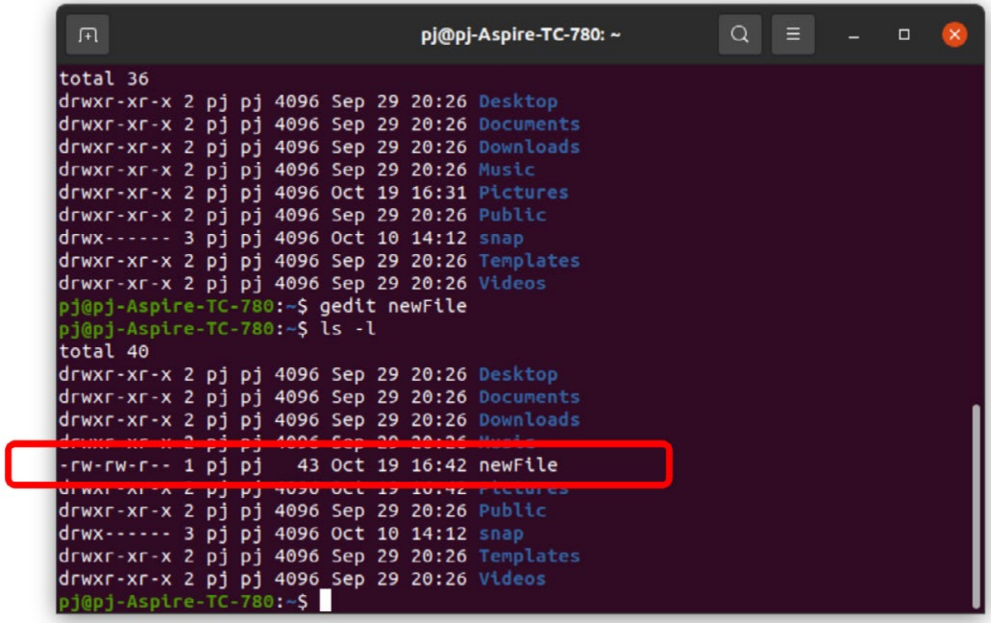


```
this is a new file set up for this example
```

Now let’s use the same command as before to view all the files and folders:

```
ls -l
```

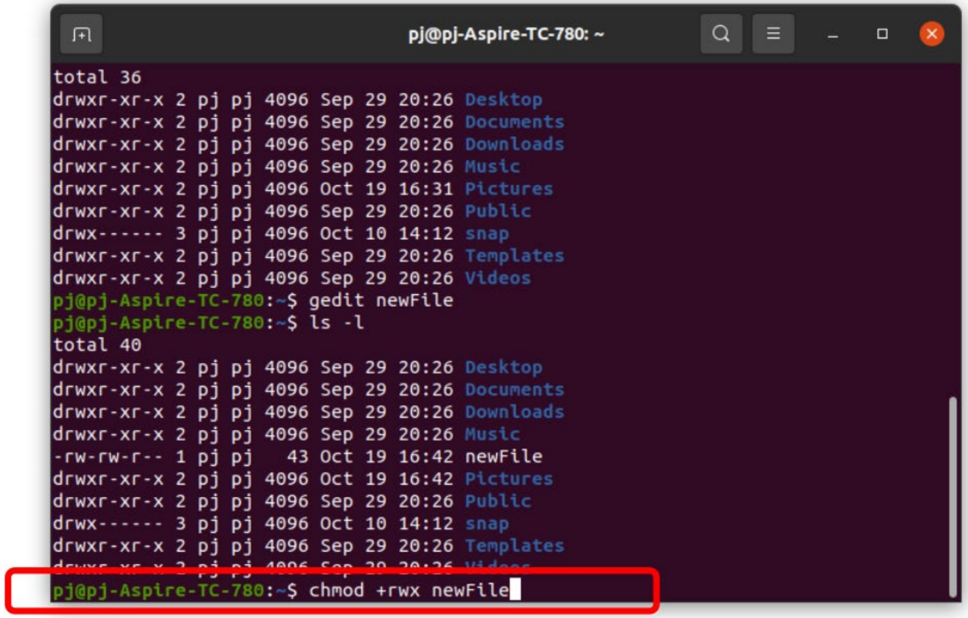
You can see that the file is now visible and the default permissions that have been placed on the file.



```
total 36
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Desktop
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Documents
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Downloads
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Music
drwxr-xr-x 2 pj pj 4096 Oct 19 16:31 Pictures
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Public
drwx------ 3 pj pj 4096 Oct 10 14:12 snap
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Templates
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Videos
pj@pj-Aspire-TC-780:~$ gedit newFile
pj@pj-Aspire-TC-780:~$ ls -l
total 40
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Desktop
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Documents
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Downloads
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Music
-rw-rw-r-- 1 pj pj   43 Oct 19 16:42 newFile
drwxr-xr-x 2 pj pj 4096 Oct 19 16:42 Pictures
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Public
drwx------ 3 pj pj 4096 Oct 10 14:12 snap
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Templates
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Videos
pj@pj-Aspire-TC-780:~$
```

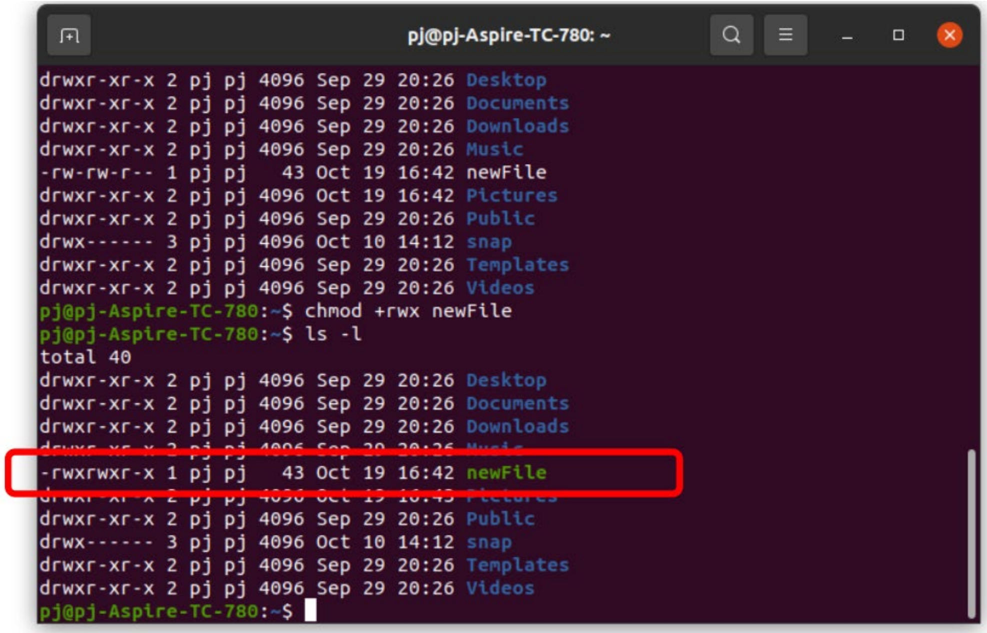
To edit the permissions of the file to **add** read, write, and execute you use the following command:

```
chmod +rwx newFile
```



```
total 36
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Desktop
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Documents
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Downloads
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Music
drwxr-xr-x 2 pj pj 4096 Oct 19 16:31 Pictures
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Public
drwx------ 3 pj pj 4096 Oct 10 14:12 snap
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Templates
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Videos
pj@pj-Aspire-TC-780:~$ gedit newFile
pj@pj-Aspire-TC-780:~$ ls -l
total 40
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Desktop
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Documents
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Downloads
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Music
-rw-rw-r-- 1 pj pj   43 Oct 19 16:42 newFile
drwxr-xr-x 2 pj pj 4096 Oct 19 16:42 Pictures
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Public
drwx------ 3 pj pj 4096 Oct 10 14:12 snap
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Templates
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Videos
pj@pj-Aspire-TC-780:~$ chmod +rwx newFile
```

View the files and folders again to see that the permissions have been amended for the new file.

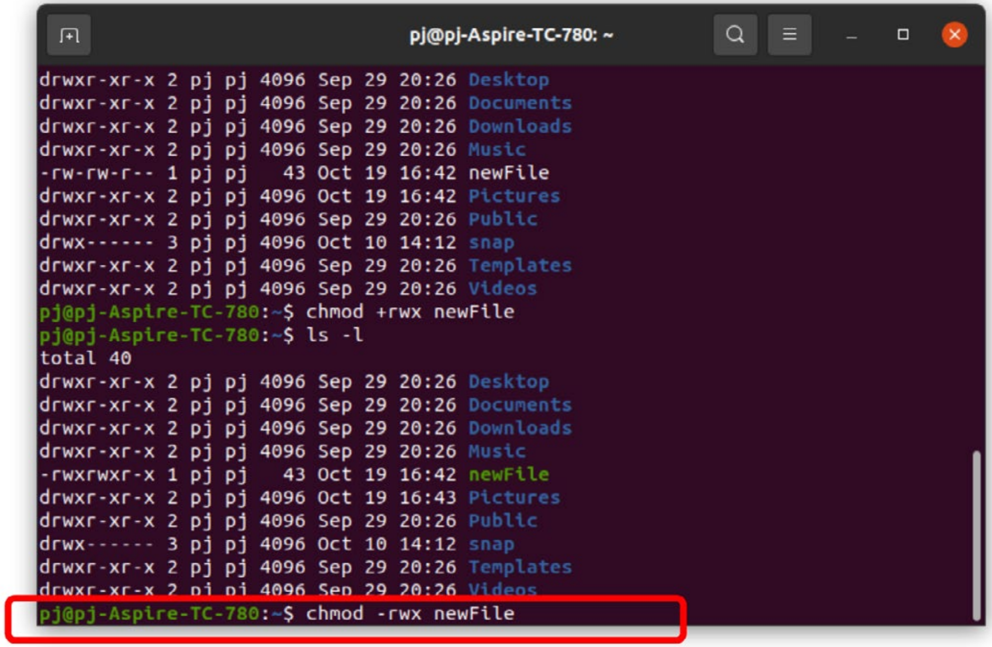


```
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Desktop
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Documents
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Downloads
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Music
-rw-rw-r-- 1 pj pj   43 Oct 19 16:42 newFile
drwxr-xr-x 2 pj pj 4096 Oct 19 16:42 Pictures
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Public
drwx------ 3 pj pj 4096 Oct 10 14:12 snap
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Templates
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Videos
pj@pj-Aspire-TC-780:~$ chmod +rwx newFile
pj@pj-Aspire-TC-780:~$ ls -l
total 40
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Desktop
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Documents
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Downloads
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Music
-rwxrwxr-x 1 pj pj   43 Oct 19 16:42 newFile
drwxr-xr-x 2 pj pj 4096 Oct 19 16:43 Pictures
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Public
drwx------ 3 pj pj 4096 Oct 10 14:12 snap
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Templates
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Videos
pj@pj-Aspire-TC-780:~$ 
```

To edit the permissions of the file to **remove** read, write, and execute you use the following command:

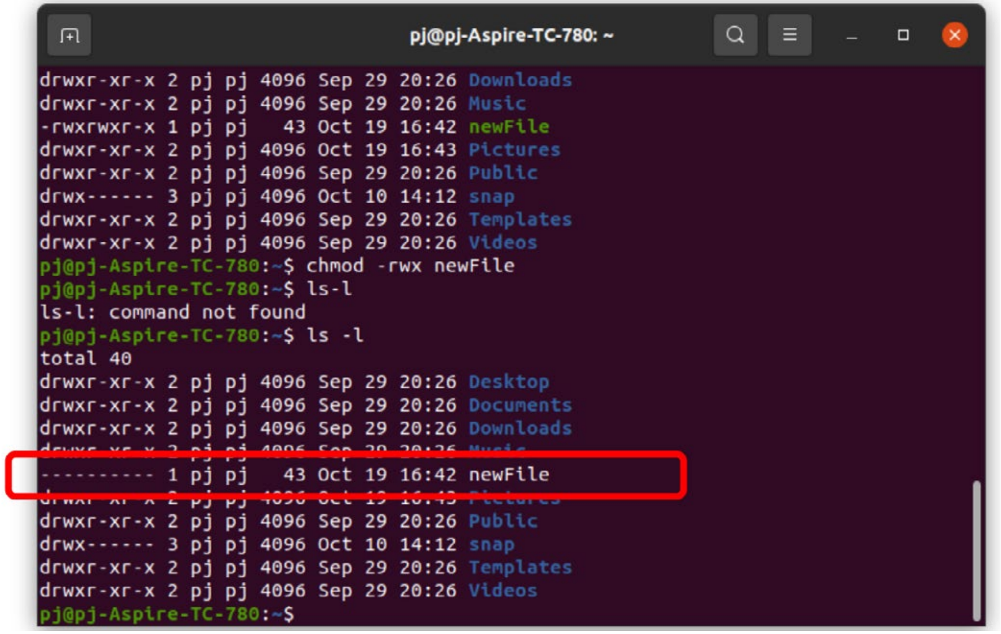
`chmod -rwx newFile`

Notice the plus sign has become a minus.



```
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Desktop
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Documents
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Downloads
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Music
-rw-rw-r-- 1 pj pj   43 Oct 19 16:42 newFile
drwxr-xr-x 2 pj pj 4096 Oct 19 16:42 Pictures
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Public
drwx------ 3 pj pj 4096 Oct 10 14:12 snap
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Templates
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Videos
pj@pj-Aspire-TC-780:~$ chmod +rwx newFile
pj@pj-Aspire-TC-780:~$ ls -l
total 40
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Desktop
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Documents
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Downloads
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Music
-rwxrwxr-x 1 pj pj   43 Oct 19 16:42 newFile
drwxr-xr-x 2 pj pj 4096 Oct 19 16:43 Pictures
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Public
drwx------ 3 pj pj 4096 Oct 10 14:12 snap
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Templates
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Videos
pj@pj-Aspire-TC-780:~$ chmod -rwx newFile
```

Use the same command line as before to now view the new permissions on the file as none:



```
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Downloads
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Music
-rwxrwxr-x 1 pj pj   43 Oct 19 16:42 newFile
drwxr-xr-x 2 pj pj 4096 Oct 19 16:43 Pictures
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Public
drwx------ 3 pj pj 4096 Oct 10 14:12 snap
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Templates
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Videos
pj@pj-Aspire-TC-780:~$ chmod -rwx newFile
pj@pj-Aspire-TC-780:~$ ls-l
ls-l: command not found
pj@pj-Aspire-TC-780:~$ ls -l
total 40
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Desktop
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Documents
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Downloads
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Music
---------- 1 pj pj   43 Oct 19 16:42 newFile
drwxr-xr-x 2 pj pj 4096 Oct 19 16:43 Pictures
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Public
drwx------ 3 pj pj 4096 Oct 10 14:12 snap
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Templates
drwxr-xr-x 2 pj pj 4096 Sep 29 20:26 Videos
pj@pj-Aspire-TC-780:~$
```

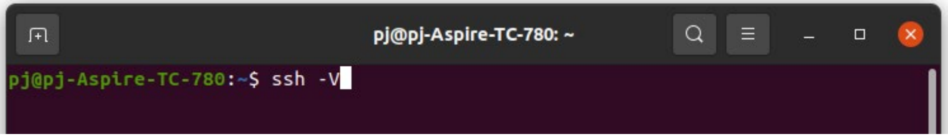
SSH Secure Shell

SSH stands for Secure Shell, and it is a network protocol. It is used to operate remote logins and commands on machines over local and remote networks. SSH is secure and encrypts data that is transmitted over the network.

Enabling and Disabling SSH

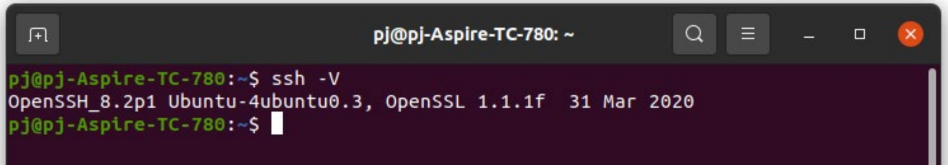
SSH should be already installed on your device, and we can check that using the following command:

```
ssh -V
```



```
pj@pj-Aspire-TC-780:~$ ssh -V
```

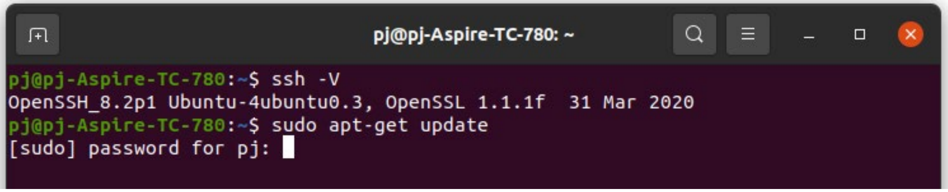
You will see a response stating that there is an application there and it was last updated on the 31st of March 2020.



```
pj@pj-Aspire-TC-780:~$ ssh -V
OpenSSH_8.2p1 Ubuntu-4ubuntu0.3, OpenSSL 1.1.1f  31 Mar 2020
pj@pj-Aspire-TC-780:~$
```

Like anything, we need to ensure that we have the most up to date version to ensure we are using a secure, up-to-date application.

```
sudo apt-get update
```

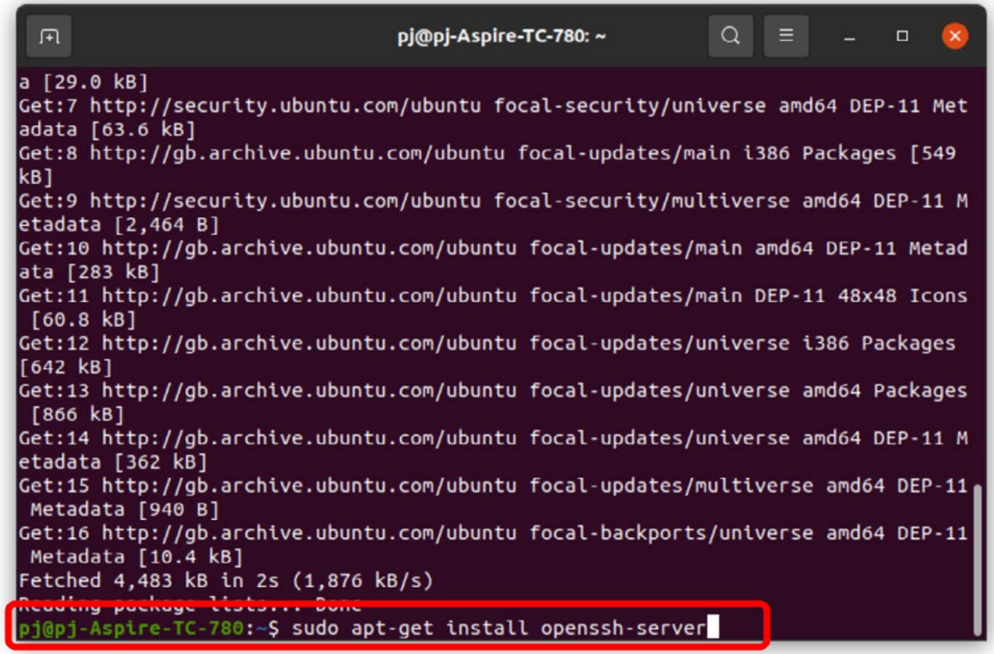


```
pj@pj-Aspire-TC-780:~$ ssh -V
OpenSSH_8.2p1 Ubuntu-4ubuntu0.3, OpenSSL 1.1.1f  31 Mar 2020
pj@pj-Aspire-TC-780:~$ sudo apt-get update
[sudo] password for pj: 
```

Once your password has been added for using the sudo permissions, you will see the system unpack the update and install the update on the system.

Now we have updated all the packages we need to install Open SSH.

```
sudo apt-get update
```

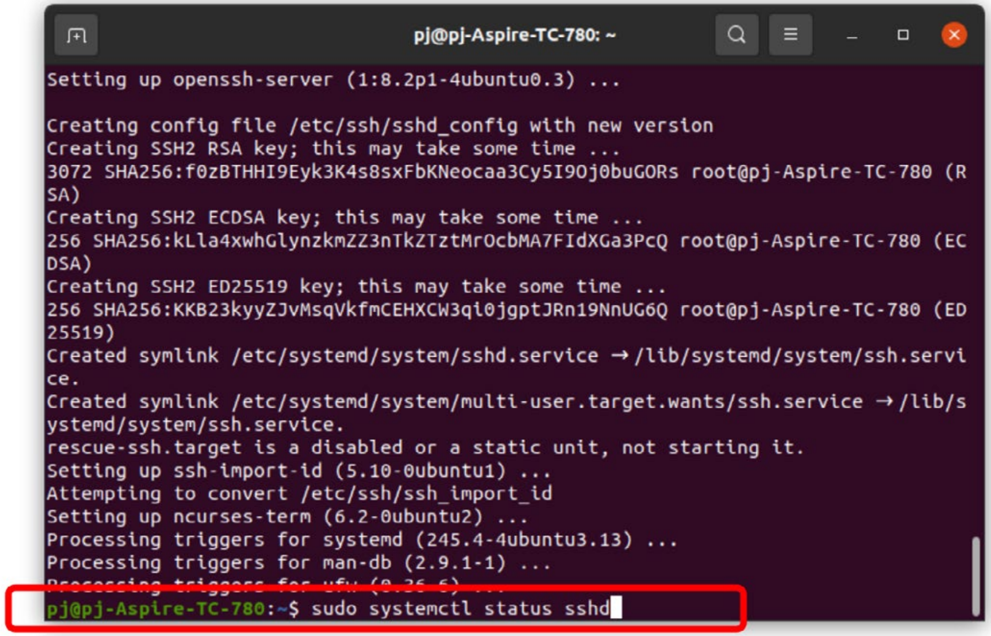


```
a [29.0 kB]
Get:7 http://security.ubuntu.com/ubuntu focal-security/universe amd64 DEP-11 Met
adata [63.6 kB]
Get:8 http://gb.archive.ubuntu.com/ubuntu focal-updates/main i386 Packages [549
kB]
Get:9 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 DEP-11 M
etadata [2,464 B]
Get:10 http://gb.archive.ubuntu.com/ubuntu focal-updates/main amd64 DEP-11 Metad
ata [283 kB]
Get:11 http://gb.archive.ubuntu.com/ubuntu focal-updates/main DEP-11 48x48 Icons
 [60.8 kB]
Get:12 http://gb.archive.ubuntu.com/ubuntu focal-updates/universe i386 Packages
[642 kB]
Get:13 http://gb.archive.ubuntu.com/ubuntu focal-updates/universe amd64 Packages
 [866 kB]
Get:14 http://gb.archive.ubuntu.com/ubuntu focal-updates/universe amd64 DEP-11 M
etadata [362 kB]
Get:15 http://gb.archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 DEP-11
 Metadata [940 B]
Get:16 http://gb.archive.ubuntu.com/ubuntu focal-backports/universe amd64 DEP-11
 Metadata [10.4 kB]
Fetched 4,483 kB in 2s (1,876 kB/s)
Reading package lists... Done
pj@pj-Aspire-TC-780:~$ sudo apt-get install openssh-server
```

Now that this has been installed you will find a configuration file created in the **/etc/ssh** folder named **sshd_config**.

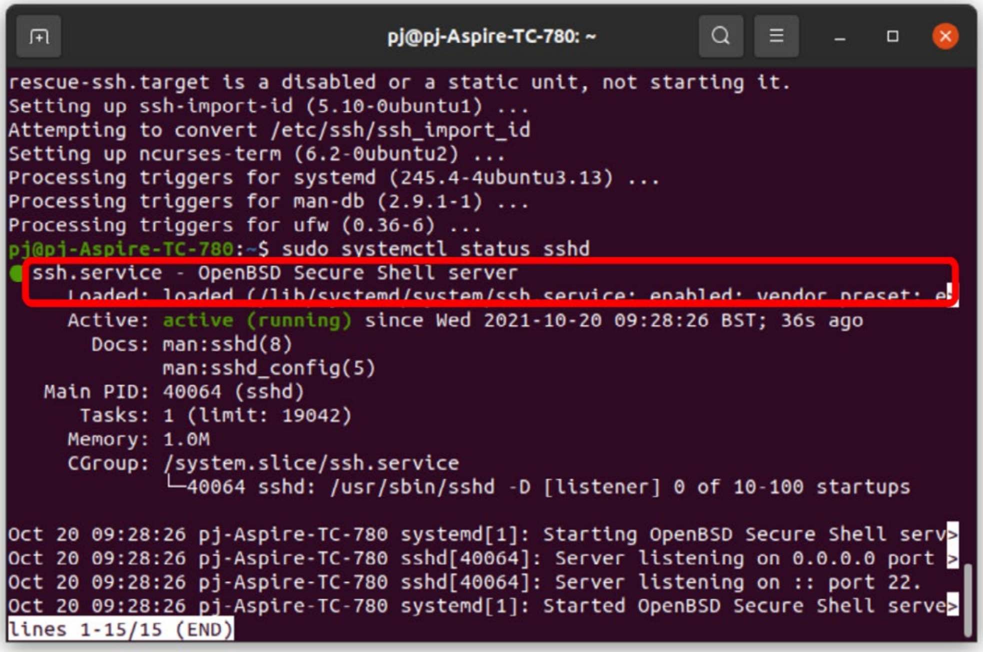
The next step is to check it is now running:

```
sudo systemctl status sshd
```



```
Setting up openssh-server (1:8.2p1-4ubuntu0.3) ...

Creating config file /etc/ssh/sshd_config with new version
Creating SSH2 RSA key; this may take some time ...
3072 SHA256:f0zBTHHI9Eyk3K4s8sxFbKNeocaa3Cy5I9Oj0buGORs root@pj-Aspire-TC-780 (R
SA)
Creating SSH2 ECDSA key; this may take some time ...
256 SHA256:kLla4xwhGlynzkmZZ3nTkZTztMrOcbMA7FIdXGa3PcQ root@pj-Aspire-TC-780 (EC
DSA)
Creating SSH2 ED25519 key; this may take some time ...
256 SHA256:KKB23kyyZJvMsqVkfmCEHXCW3qi0jgptJRn19NnUG6Q root@pj-Aspire-TC-780 (ED
25519)
Created symlink /etc/systemd/system/sshd.service → /lib/systemd/system/ssh.servi
ce.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /lib/s
ystemd/system/ssh.service.
rescue-ssh.target is a disabled or a static unit, not starting it.
Setting up ssh-import-id (5.10-0ubuntu1) ...
Attempting to convert /etc/ssh/ssh_import_id
Setting up ncurses-term (6.2-0ubuntu2) ...
Processing triggers for systemd (245.4-4ubuntu3.13) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for ufw (0.36-6) ...
pj@pj-Aspire-TC-780:~$ sudo systemctl status sshd
```

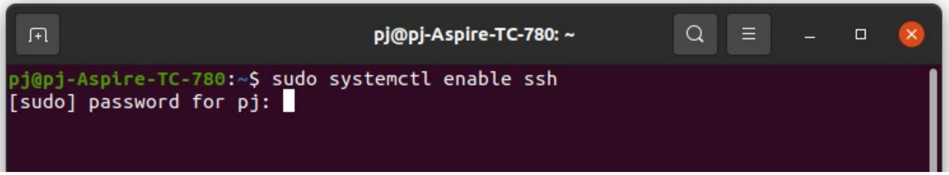
You will see the active row that shows that this is now running, and this means that the SSH is now running as a service on the device.



```
rescue-ssh.target is a disabled or a static unit, not starting it.
Setting up ssh-import-id (5.10-0ubuntu1) ...
Attempting to convert /etc/ssh/ssh_import_id
Setting up ncurses-term (6.2-0ubuntu2) ...
Processing triggers for systemd (245.4-4ubuntu3.13) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for ufw (0.36-6) ...
pj@pj-Aspire-TC-780:~$ sudo systemctl status sshd
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: e>
     Active: active (running) since Wed 2021-10-20 09:28:26 BST; 36s ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 40064 (sshd)
      Tasks: 1 (limit: 19042)
     Memory: 1.0M
     CGroup: /system.slice/ssh.service
             └─40064 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Oct 20 09:28:26 pj-Aspire-TC-780 systemd[1]: Starting OpenBSD Secure Shell serv>
Oct 20 09:28:26 pj-Aspire-TC-780 sshd[40064]: Server listening on 0.0.0.0 port >
Oct 20 09:28:26 pj-Aspire-TC-780 sshd[40064]: Server listening on :: port 22.
Oct 20 09:28:26 pj-Aspire-TC-780 systemd[1]: Started OpenBSD Secure Shell serve>
lines 1-15/15 (END)
```

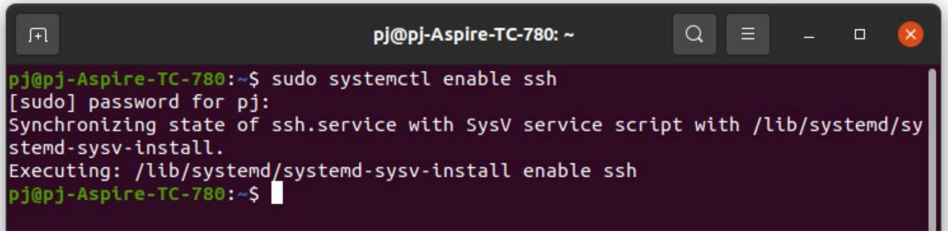
To enable the SSH to be launched at boot time use the command:

`sudo systemctl enable ssh`



```
pj@pj-Aspire-TC-780:~$ sudo systemctl enable ssh
[sudo] password for pj: █
```

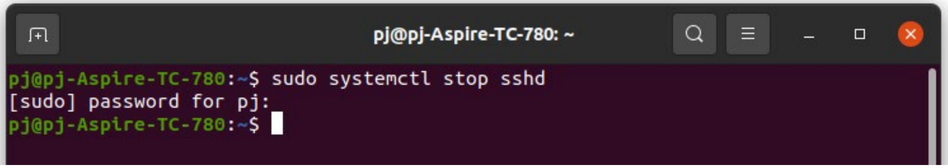
Once you have entered your password you will see the below showing that the SSH has been enabled.



```
pj@pj-Aspire-TC-780:~$ sudo systemctl enable ssh
[sudo] password for pj:
Synchronizing state of ssh.service with SysV service script with /lib/systemd/sy
stemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable ssh
pj@pj-Aspire-TC-780:~$ █
```

To **disable** the SSH server you need to use the command:

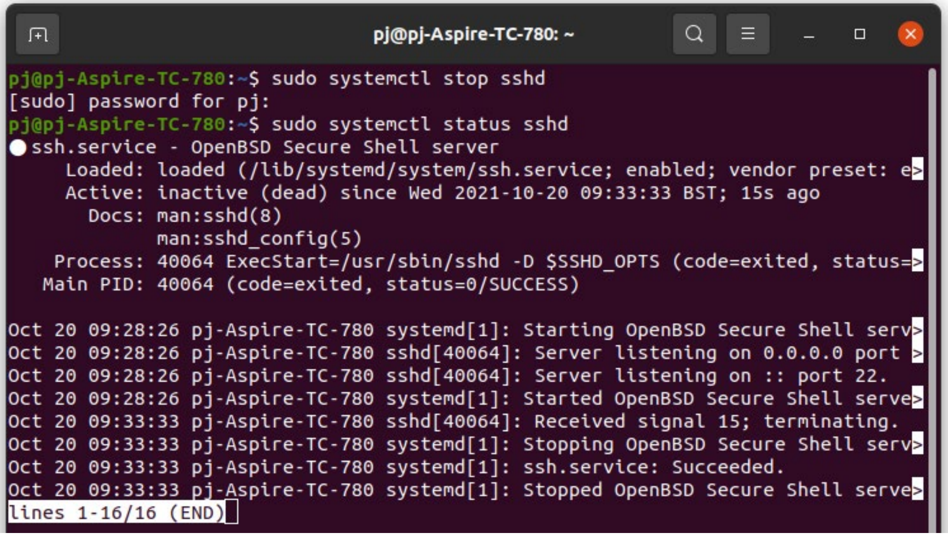
`sudo systemctl stop sshd`



```
pj@pj-Aspire-TC-780:~$ sudo systemctl stop sshd
[sudo] password for pj:
pj@pj-Aspire-TC-780:~$ █
```

Use the check status command to check it has been disabled.

`sudo systemctl status sshd`



```
pj@pj-Aspire-TC-780:~$ sudo systemctl stop sshd
[sudo] password for pj:
pj@pj-Aspire-TC-780:~$ sudo systemctl status sshd
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: e>
     Active: inactive (dead) since Wed 2021-10-20 09:33:33 BST; 15s ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 40064 ExecStart=/usr/sbin/sshd -D $SSHD_OPTS (code=exited, status=>
   Main PID: 40064 (code=exited, status=0/SUCCESS)

Oct 20 09:28:26 pj-Aspire-TC-780 systemd[1]: Starting OpenBSD Secure Shell serv>
Oct 20 09:28:26 pj-Aspire-TC-780 sshd[40064]: Server listening on 0.0.0.0 port >
Oct 20 09:28:26 pj-Aspire-TC-780 sshd[40064]: Server listening on :: port 22.
Oct 20 09:28:26 pj-Aspire-TC-780 systemd[1]: Started OpenBSD Secure Shell serve>
Oct 20 09:33:33 pj-Aspire-TC-780 sshd[40064]: Received signal 15; terminating.
Oct 20 09:33:33 pj-Aspire-TC-780 systemd[1]: Stopping OpenBSD Secure Shell serv>
Oct 20 09:33:33 pj-Aspire-TC-780 systemd[1]: ssh.service: Succeeded.
Oct 20 09:33:33 pj-Aspire-TC-780 systemd[1]: Stopped OpenBSD Secure Shell serve>
lines 1-16/16 (END)
```

Auditing

The aim of auditing settings is to identify attacks that are both successful and not, that could be a threat to your device and/or network.

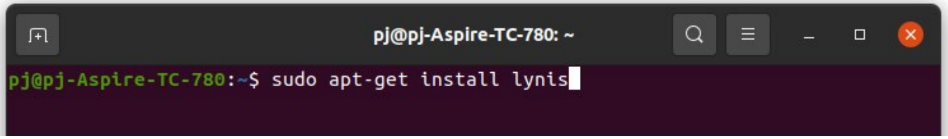
For example, identifying successful and failed logins can help identify when a user has accessed their account to identify a suspicious login outside of known logins as well as attempts to hack into the account logged as failed attempts.

By default, all auditing tools are disabled when first installed and if you are considering using these tools, they will need to be enabled.

Lynis is an open-source security tool. It helps with auditing systems running UNIX-alike systems (Linux, macOS, BSD), and providing guidance for system hardening and compliance testing.

First, we need to install this application to be able to use it, use the command line:

```
apt-get install lynis
```

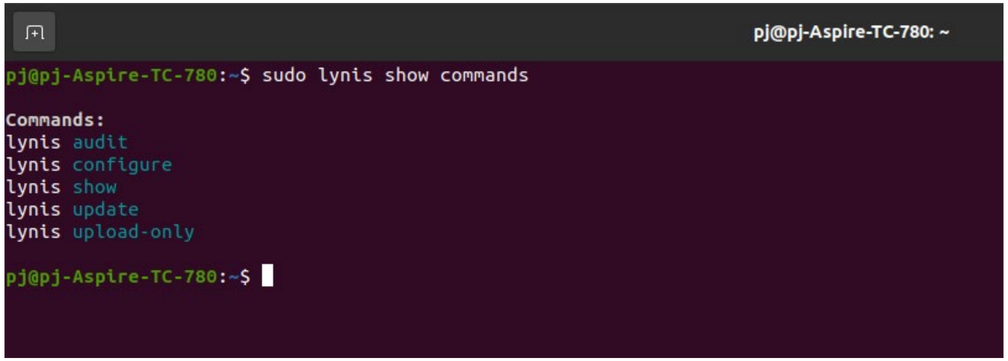


```
pj@pj-Aspire-TC-780:~$ sudo apt-get install lynis
```

The application will be unpacked and when prompted add **Y** and press enter to install the full package.

Let's look at the commands that can be used, you can ask this question using the command:

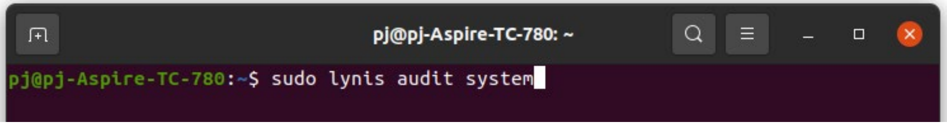
```
sudo lynis show commands
```



```
pj@pj-Aspire-TC-780:~$ sudo lynis show commands

Commands:
lynis audit
lynis configure
lynis show
lynis update
lynis upload-only

pj@pj-Aspire-TC-780:~$
```

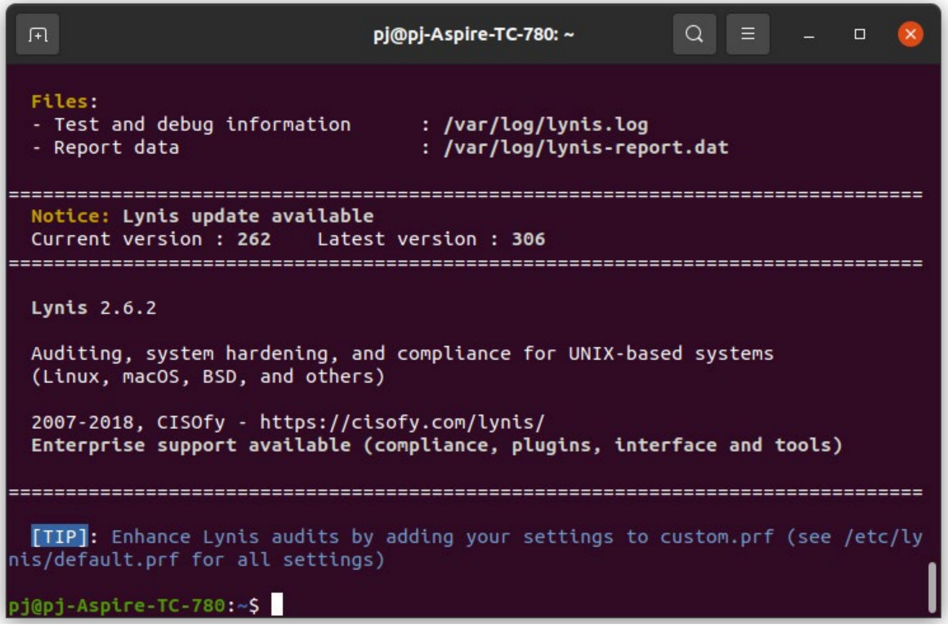
Now we can look at using this for an audit of the system by using the command:

```
sudo lynis audit system
```

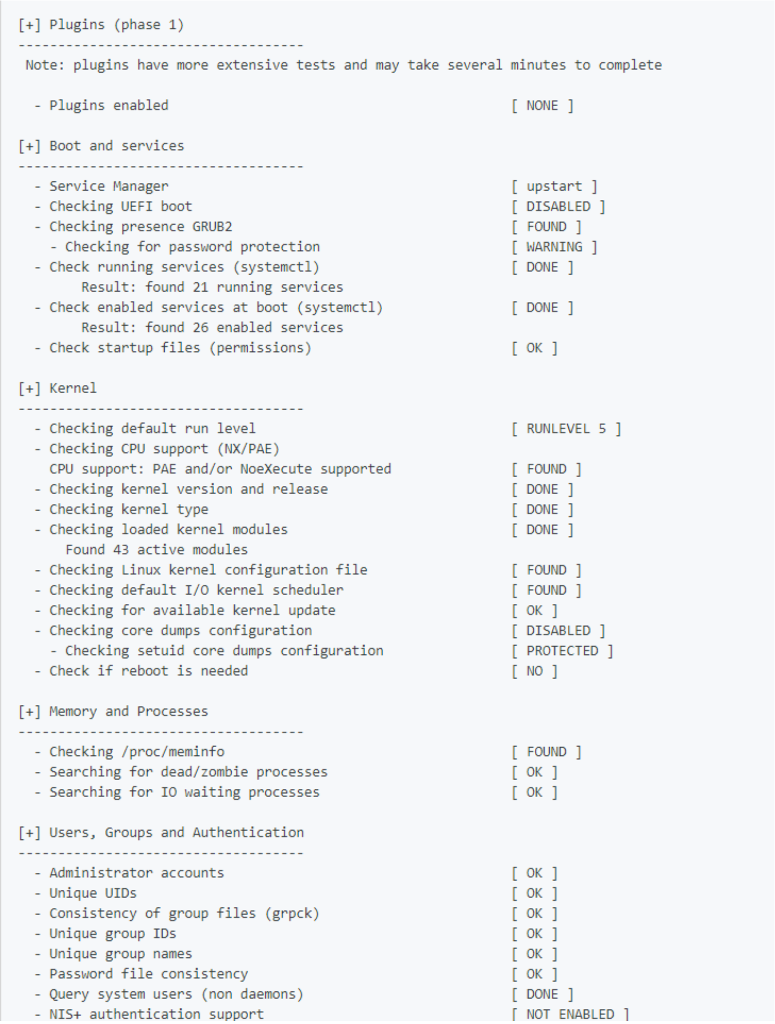


```
pj@pj-Aspire-TC-780:~$ sudo lynis audit system
```

When this runs the system is audited and the process will show many lines of information.



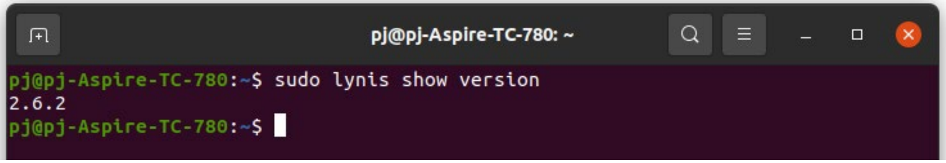
```
  Files:
  - Test and debug information      : /var/log/lynis.log
  - Report data                     : /var/log/lynis-report.dat

================================================================================
  Notice: Lynis update available
  Current version : 262    Latest version : 306
================================================================================

  Lynis 2.6.2

  Auditing, system hardening, and compliance for UNIX-based systems
  (Linux, macOS, BSD, and others)

  2007-2018, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)

================================================================================

  [TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /etc/ly
nis/default.prf for all settings)

pj@pj-Aspire-TC-780:~$
```



```
[+] Plugins (phase 1)
------------------------------------
 Note: plugins have more extensive tests and may take several minutes to complete

  - Plugins enabled                                           [ NONE ]

[+] Boot and services
------------------------------------
  - Service Manager                                           [ upstart ]
  - Checking UEFI boot                                        [ DISABLED ]
  - Checking presence GRUB2                                   [ FOUND ]
    - Checking for password protection                        [ WARNING ]
  - Check running services (systemctl)                        [ DONE ]
      Result: found 21 running services
  - Check enabled services at boot (systemctl)                [ DONE ]
      Result: found 26 enabled services
  - Check startup files (permissions)                         [ OK ]

[+] Kernel
------------------------------------
  - Checking default run level                                [ RUNLEVEL 5 ]
  - Checking CPU support (NX/PAE)
    CPU support: PAE and/or NoeXecute supported               [ FOUND ]
  - Checking kernel version and release                       [ DONE ]
  - Checking kernel type                                      [ DONE ]
  - Checking loaded kernel modules                            [ DONE ]
      Found 43 active modules
  - Checking Linux kernel configuration file                  [ FOUND ]
  - Checking default I/O kernel scheduler                     [ FOUND ]
  - Checking for available kernel update                      [ OK ]
  - Checking core dumps configuration                         [ DISABLED ]
    - Checking setuid core dumps configuration                [ PROTECTED ]
  - Check if reboot is needed                                 [ NO ]

[+] Memory and Processes
------------------------------------
  - Checking /proc/meminfo                                    [ FOUND ]
  - Searching for dead/zombie processes                       [ OK ]
  - Searching for IO waiting processes                        [ OK ]

[+] Users, Groups and Authentication
------------------------------------
  - Administrator accounts                                    [ OK ]
  - Unique UIDs                                               [ OK ]
  - Consistency of group files (grpck)                        [ OK ]
  - Unique group IDs                                          [ OK ]
  - Unique group names                                        [ OK ]
  - Password file consistency                                 [ OK ]
  - Query system users (non daemons)                          [ DONE ]
  - NIS+ authentication support                               [ NOT ENABLED ]
```

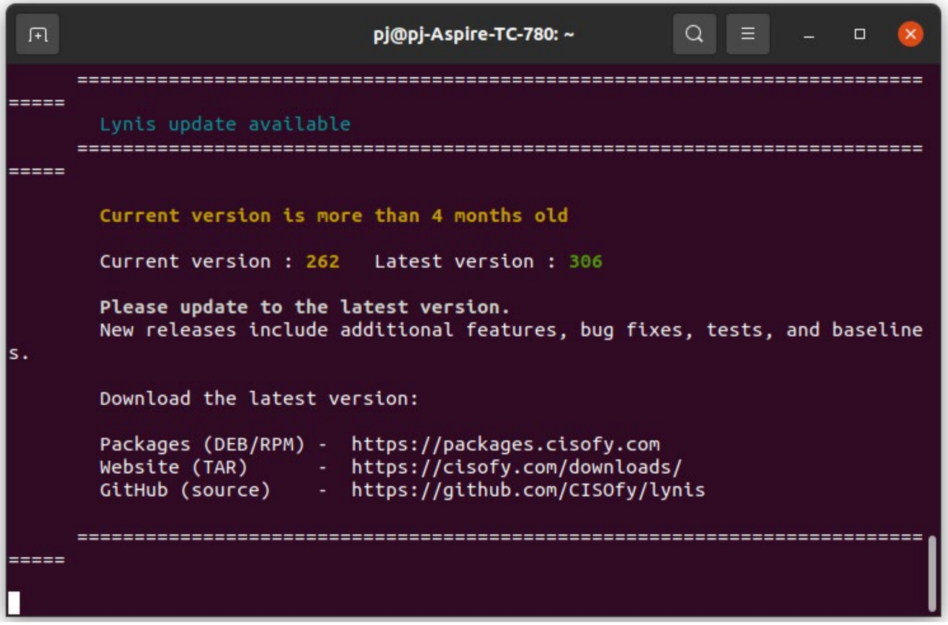
One aspect is that the version that is installed is version 2.6.2. You can check the install version by using the command:

```
sudo lynis show version
```



```
pj@pj-Aspire-TC-780:~$ sudo lynis show version
2.6.2
pj@pj-Aspire-TC-780:~$ 
```

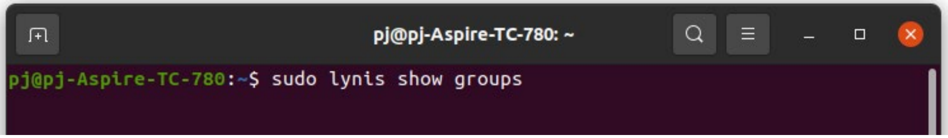
The version installed by default is version 2.6.2 and to update you need to follow the details on there to download and install any updates.



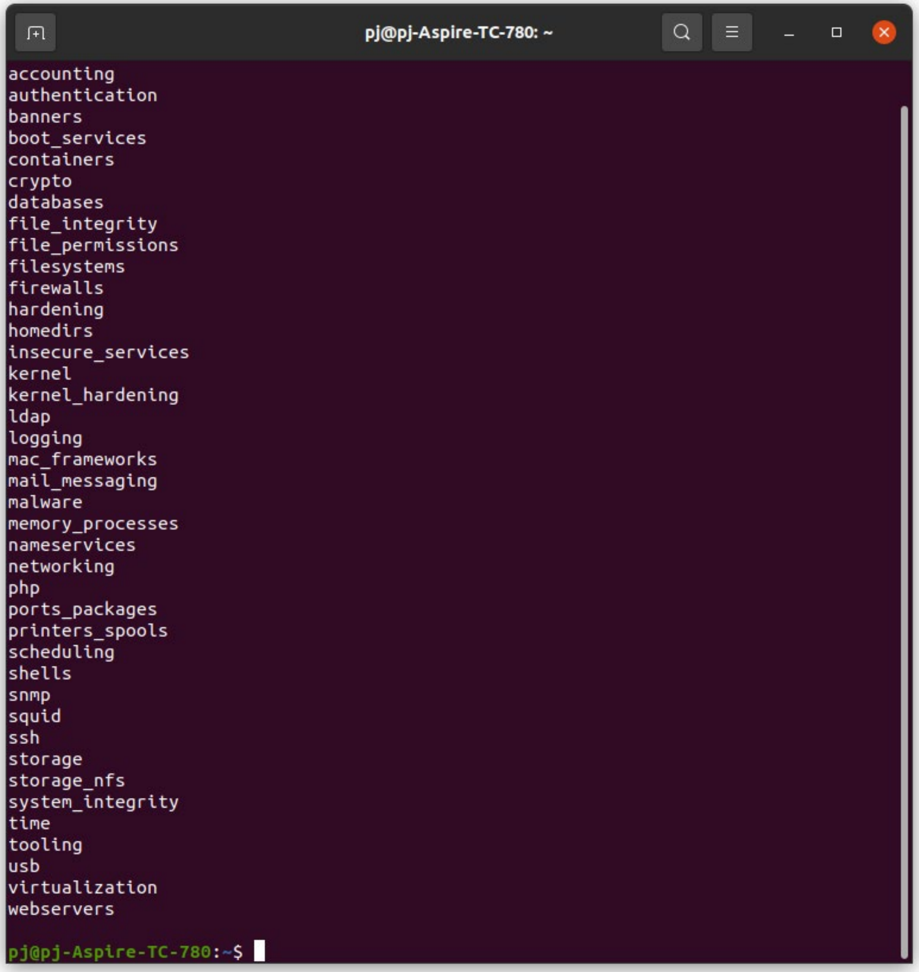
```
        ========================================================================
=====

        Lynis update available
        ========================================================================
=====

        Current version is more than 4 months old

        Current version : 262   Latest version : 306

        Please update to the latest version.
        New releases include additional features, bug fixes, tests, and baseline
s.

        Download the latest version:

        Packages (DEB/RPM) -  https://packages.cisofy.com
        Website (TAR)      -  https://cisofy.com/downloads/
        GitHub (source)    -  https://github.com/CISOfy/lynis

        ========================================================================
=====
```

When you use this command, it generate a lot to look through. You can scan the system by groups, to list all possible groups use the command:

```
sudo lynis show groups
```



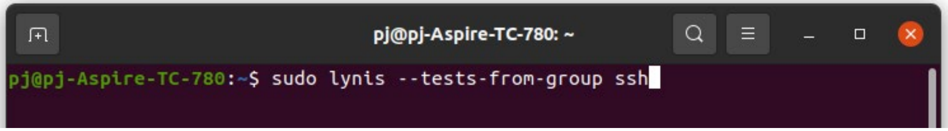
```
pj@pj-Aspire-TC-780:~$ sudo lynis show groups
```



```
accounting
authentication
banners
boot_services
containers
crypto
databases
file_integrity
file_permissions
filesystems
firewalls
hardening
homedirs
insecure_services
kernel
kernel_hardening
ldap
logging
mac_frameworks
mail_messaging
malware
memory_processes
nameservices
networking
php
ports_packages
printers_spools
scheduling
shells
snmp
squid
ssh
storage
storage_nfs
system_integrity
time
tooling
usb
virtualization
webservers

pj@pj-Aspire-TC-780:~$
```

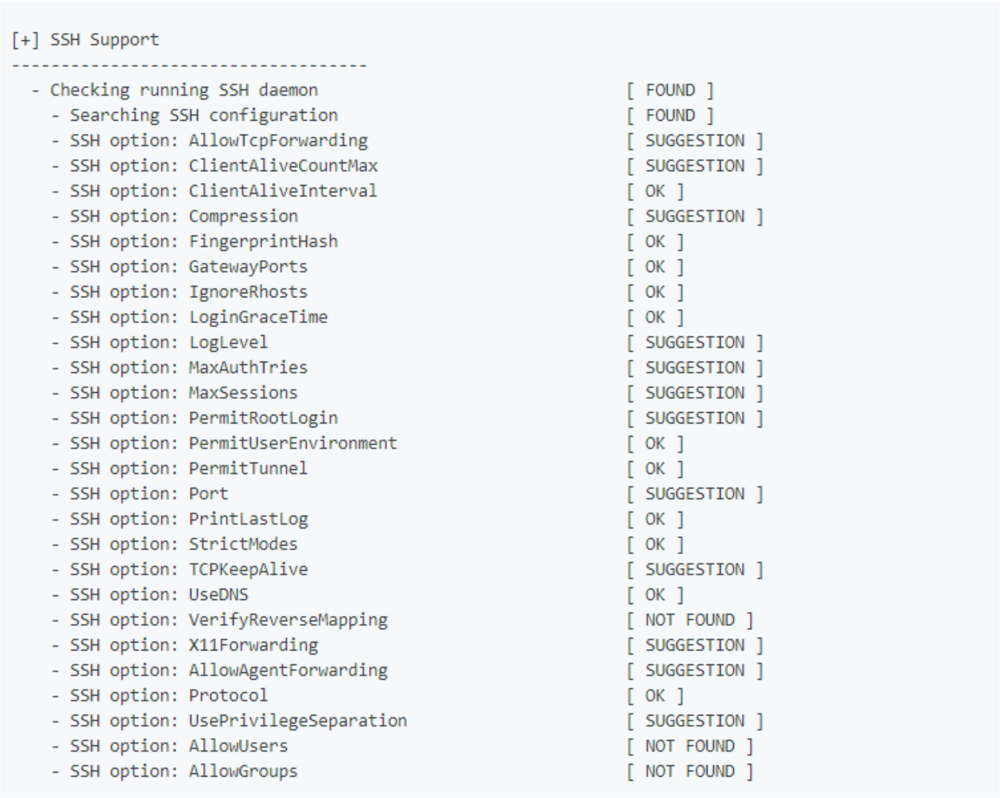
You can then use the following command line to complete an audit on a specific folder:

```
sudo lynis –tests-from-group ssh
```



```
pj@pj-Aspire-TC-780:~$ sudo lynis --tests-from-group ssh
```

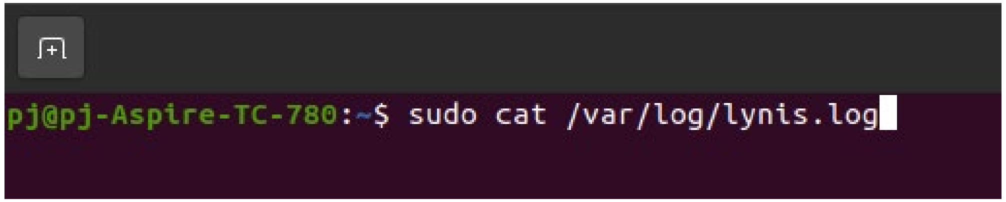
An example of the type of output you will see is on the right.



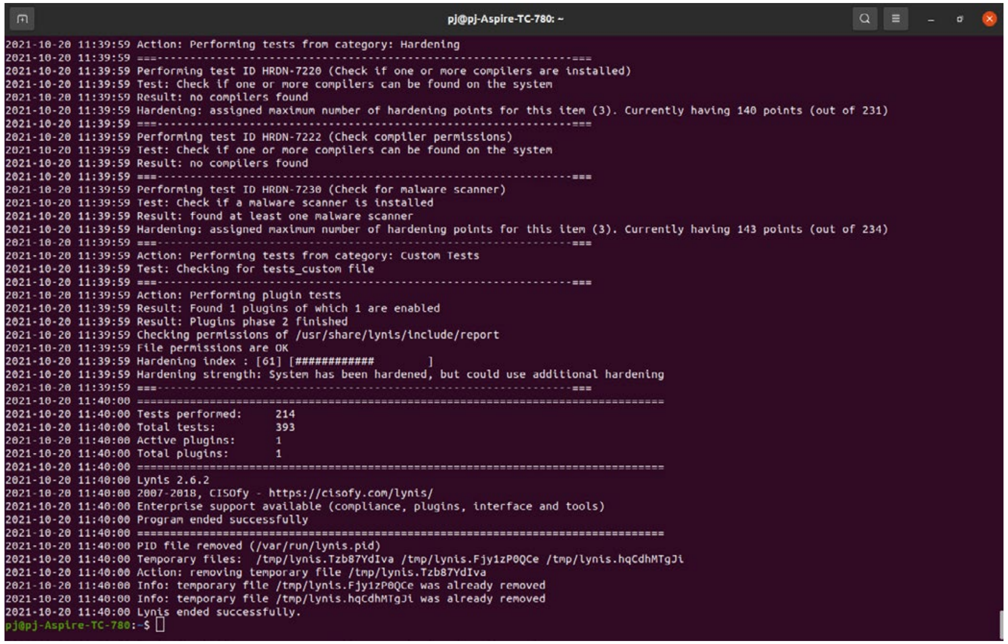
```
[+] SSH Support
------------------------------------
  - Checking running SSH daemon                          [ FOUND ]
    - Searching SSH configuration                        [ FOUND ]
    - SSH option: AllowTcpForwarding                     [ SUGGESTION ]
    - SSH option: ClientAliveCountMax                    [ SUGGESTION ]
    - SSH option: ClientAliveInterval                    [ OK ]
    - SSH option: Compression                            [ SUGGESTION ]
    - SSH option: FingerprintHash                        [ OK ]
    - SSH option: GatewayPorts                           [ OK ]
    - SSH option: IgnoreRhosts                           [ OK ]
    - SSH option: LoginGraceTime                         [ OK ]
    - SSH option: LogLevel                               [ SUGGESTION ]
    - SSH option: MaxAuthTries                           [ SUGGESTION ]
    - SSH option: MaxSessions                            [ SUGGESTION ]
    - SSH option: PermitRootLogin                        [ SUGGESTION ]
    - SSH option: PermitUserEnvironment                  [ OK ]
    - SSH option: PermitTunnel                           [ OK ]
    - SSH option: Port                                   [ SUGGESTION ]
    - SSH option: PrintLastLog                           [ OK ]
    - SSH option: StrictModes                            [ OK ]
    - SSH option: TCPKeepAlive                           [ SUGGESTION ]
    - SSH option: UseDNS                                 [ OK ]
    - SSH option: VerifyReverseMapping                   [ NOT FOUND ]
    - SSH option: X11Forwarding                          [ SUGGESTION ]
    - SSH option: AllowAgentForwarding                   [ SUGGESTION ]
    - SSH option: Protocol                               [ OK ]
    - SSH option: UsePrivilegeSeparation                 [ SUGGESTION ]
    - SSH option: AllowUsers                             [ NOT FOUND ]
    - SSH option: AllowGroups                            [ NOT FOUND ]
```

To view the audit log that is created when running an audit of the system, you use the command:

```
sudo cat /var/log/lynis.log
```



```
pj@pj-Aspire-TC-780:~$ sudo cat /var/log/lynis.log
```



```
2021-10-20 11:39:59 Action: Performing tests from category: Hardening
2021-10-20 11:39:59 ===---------------------------------------------------------------===
2021-10-20 11:39:59 Performing test ID HRDN-7220 (Check if one or more compilers are installed)
2021-10-20 11:39:59 Test: Check if one or more compilers can be found on the system
2021-10-20 11:39:59 Result: no compilers found
2021-10-20 11:39:59 Hardening: assigned maximum number of hardening points for this item (3). Currently having 140 points (out of 231)
2021-10-20 11:39:59 ===---------------------------------------------------------------===
2021-10-20 11:39:59 Performing test ID HRDN-7222 (Check compiler permissions)
2021-10-20 11:39:59 Test: Check if one or more compilers can be found on the system
2021-10-20 11:39:59 Result: no compilers found
2021-10-20 11:39:59 ===---------------------------------------------------------------===
2021-10-20 11:39:59 Performing test ID HRDN-7230 (Check for malware scanner)
2021-10-20 11:39:59 Test: Check if a malware scanner is installed
2021-10-20 11:39:59 Result: found at least one malware scanner
2021-10-20 11:39:59 Hardening: assigned maximum number of hardening points for this item (3). Currently having 143 points (out of 234)
2021-10-20 11:39:59 ===---------------------------------------------------------------===
2021-10-20 11:39:59 Action: Performing tests from category: Custom Tests
2021-10-20 11:39:59 Test: Checking for tests_custom file
2021-10-20 11:39:59 ===---------------------------------------------------------------===
2021-10-20 11:39:59 Action: Performing plugin tests
2021-10-20 11:39:59 Result: Found 1 plugins of which 1 are enabled
2021-10-20 11:39:59 Result: Plugins phase 2 finished
2021-10-20 11:39:59 Checking permissions of /usr/share/lynis/include/report
2021-10-20 11:39:59 File permissions are OK
2021-10-20 11:39:59 Hardening index : [61] [############        ]
2021-10-20 11:39:59 Hardening strength: System has been hardened, but could use additional hardening
2021-10-20 11:39:59 ===---------------------------------------------------------------===
2021-10-20 11:40:00 ================================================================================
2021-10-20 11:40:00 Tests performed:     214
2021-10-20 11:40:00 Total tests:         393
2021-10-20 11:40:00 Active plugins:      1
2021-10-20 11:40:00 Total plugins:       1
2021-10-20 11:40:00 ================================================================================
2021-10-20 11:40:00 Lynis 2.6.2
2021-10-20 11:40:00 2007-2018, CISOfy - https://cisofy.com/lynis/
2021-10-20 11:40:00 Enterprise support available (compliance, plugins, interface and tools)
2021-10-20 11:40:00 Program ended successfully
2021-10-20 11:40:00 ================================================================================
2021-10-20 11:40:00 PID file removed (/var/run/lynis.pid)
2021-10-20 11:40:00 Temporary files:  /tmp/lynis.Tzb87YdIva /tmp/lynis.Fjy1zP0QCe /tmp/lynis.hqCdhMTgJi
2021-10-20 11:40:00 Action: removing temporary file /tmp/lynis.Tzb87YdIva
2021-10-20 11:40:00 Info: temporary file /tmp/lynis.Fjy1zP0QCe was already removed
2021-10-20 11:40:00 Info: temporary file /tmp/lynis.hqCdhMTgJi was already removed
2021-10-20 11:40:00 Lynis ended successfully.
pj@pj-Aspire-TC-780:~$ 
```

You can then look through at the different areas in detail. There is information in this file that shows what was run in the background and can be used to find anomalies to rectify within the different groups.

For more information about Lynis click here.

Webmin

Webmin is an opensource web administration tool that allows users to easily monitor and manage servers.

Some of the tasks that you can accomplish with Webmin include:

- Adding and removing users on the system
- Changing users' passwords.
- Installing, updating, and removing software packages.
- Setting up a firewall.
- Configuring disk quotas to manage the space used by other users.
- Creating virtual hosts (If a web server is installed).

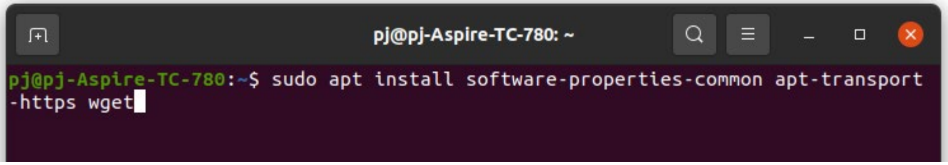
Installing Webmin

There are series of steps to follow to install and use Webmin.

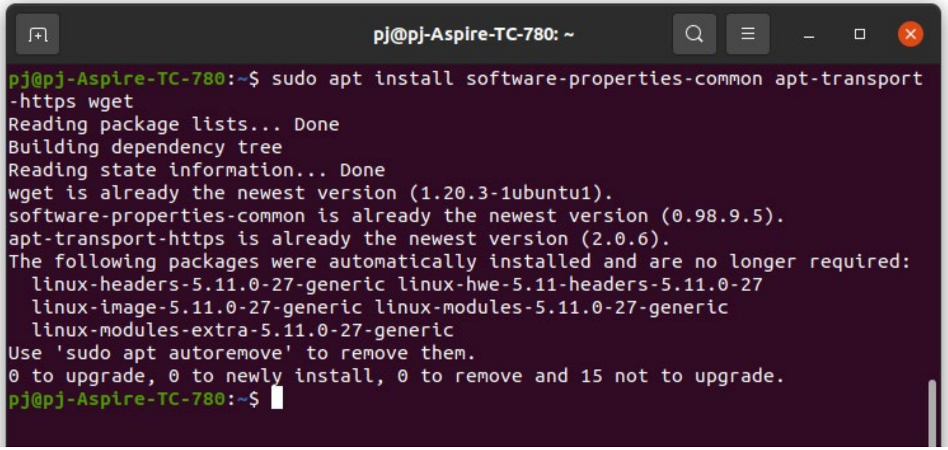
Step 1

It is always best practice to ensure you have the most up to date version of Ubuntu and run an update followed by the second command to install dependencies.

```
sudo apt update
sudo apt install software-properties-common apt-transport-https wget
```



```
pj@pj-Aspire-TC-780:~$ sudo apt install software-properties-common apt-transport
-https wget
```



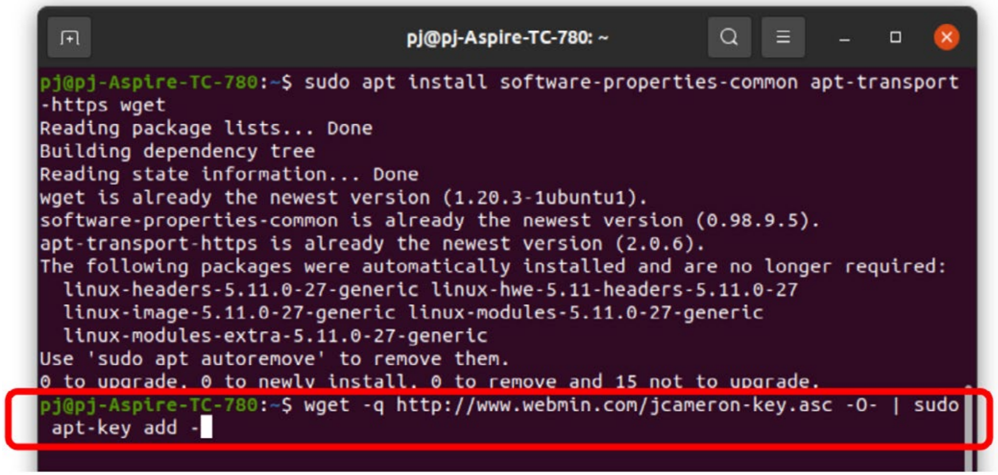
```
pj@pj-Aspire-TC-780:~$ sudo apt install software-properties-common apt-transport
-https wget
Reading package lists... Done
Building dependency tree
Reading state information... Done
wget is already the newest version (1.20.3-1ubuntu1).
software-properties-common is already the newest version (0.98.9.5).
apt-transport-https is already the newest version (2.0.6).
The following packages were automatically installed and are no longer required:
  linux-headers-5.11.0-27-generic linux-hwe-5.11-headers-5.11.0-27
  linux-image-5.11.0-27-generic linux-modules-5.11.0-27-generic
  linux-modules-extra-5.11.0-27-generic
Use 'sudo apt autoremove' to remove them.
0 to upgrade, 0 to newly install, 0 to remove and 15 not to upgrade.
pj@pj-Aspire-TC-780:~$
```

Step 2

We next need to install the Webmin GPG key and the Webmin repository to the system's software sources. To do this we use the command all on one line:

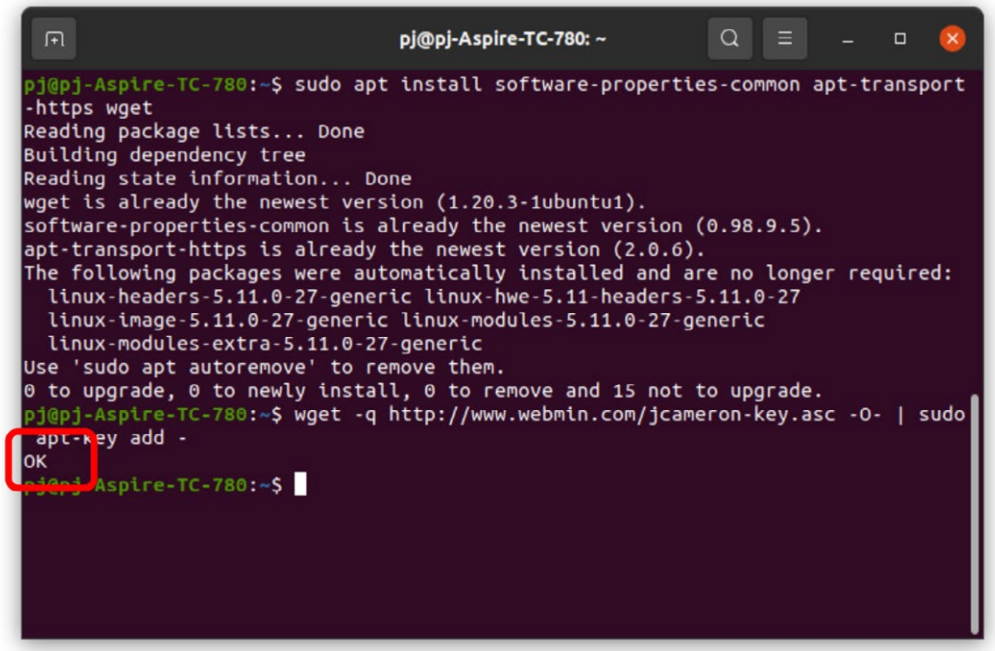
```
wget -q http://www.webmin.com/jcameron-key.asc -O- |
sudo apt-key add -
```

To get the | symbol, it is called the pipe and is located next to the left shift key on your keyboard. You need to use `shift and |` to add it.



```
pj@pj-Aspire-TC-780:~$ sudo apt install software-properties-common apt-transport
-https wget
Reading package lists... Done
Building dependency tree
Reading state information... Done
wget is already the newest version (1.20.3-1ubuntu1).
software-properties-common is already the newest version (0.98.9.5).
apt-transport-https is already the newest version (2.0.6).
The following packages were automatically installed and are no longer required:
  linux-headers-5.11.0-27-generic linux-hwe-5.11-headers-5.11.0-27
  linux-image-5.11.0-27-generic linux-modules-5.11.0-27-generic
  linux-modules-extra-5.11.0-27-generic
Use 'sudo apt autoremove' to remove them.
0 to upgrade, 0 to newly install, 0 to remove and 15 not to upgrade.
pj@pj-Aspire-TC-780:~$ wget -q http://www.webmin.com/jcameron-key.asc -O- | sudo
 apt-key add -
```

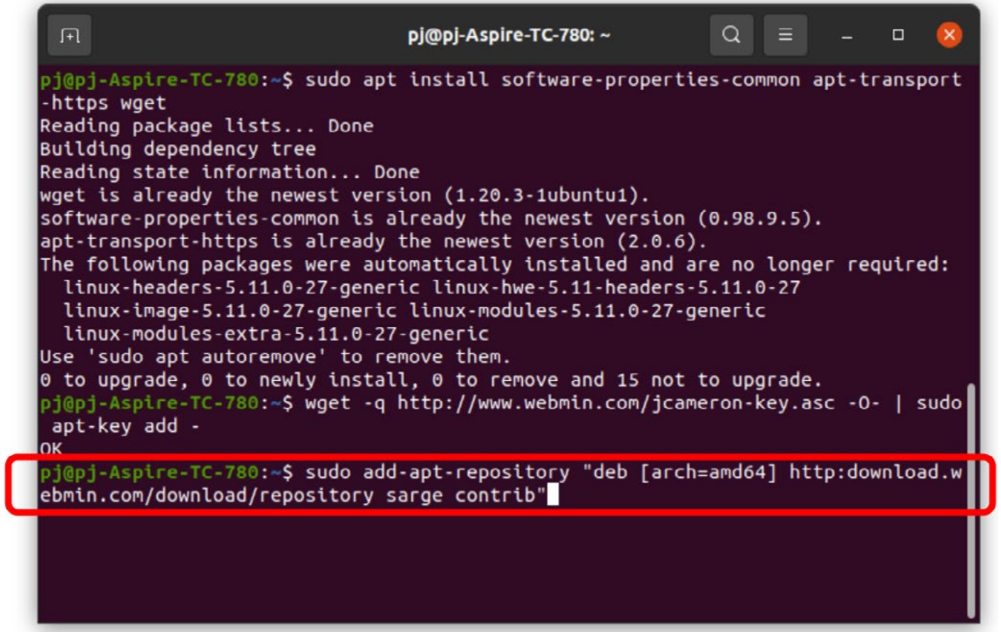
When you press enter you will receive an **OK** as a response.



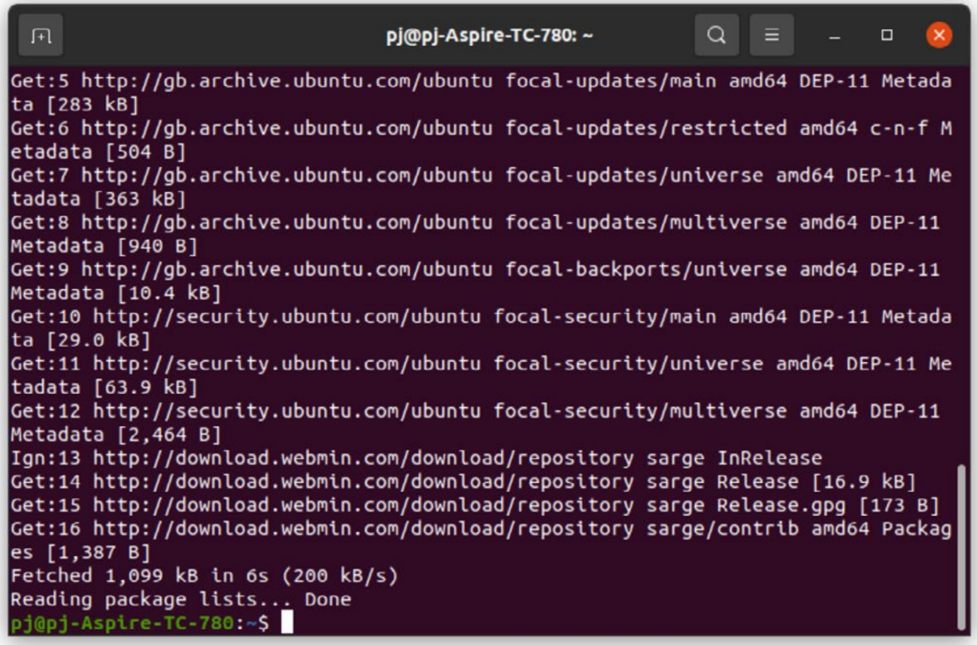
```
pj@pj-Aspire-TC-780:~$ sudo apt install software-properties-common apt-transport
-https wget
Reading package lists... Done
Building dependency tree
Reading state information... Done
wget is already the newest version (1.20.3-1ubuntu1).
software-properties-common is already the newest version (0.98.9.5).
apt-transport-https is already the newest version (2.0.6).
The following packages were automatically installed and are no longer required:
  linux-headers-5.11.0-27-generic linux-hwe-5.11-headers-5.11.0-27
  linux-image-5.11.0-27-generic linux-modules-5.11.0-27-generic
  linux-modules-extra-5.11.0-27-generic
Use 'sudo apt autoremove' to remove them.
0 to upgrade, 0 to newly install, 0 to remove and 15 not to upgrade.
pj@pj-Aspire-TC-780:~$ wget -q http://www.webmin.com/jcameron-key.asc -O- | sudo
 apt-key add -
OK
pj@pj-Aspire-TC-780:~$
```

Next add the following command, again all on one line.

```
sudo add-apt-repository “deb [arch=amd64]
http://download.webmin.com/download/repository sarge
contrib”
```



```
pj@pj-Aspire-TC-780:~$ sudo apt install software-properties-common apt-transport
-https wget
Reading package lists... Done
Building dependency tree
Reading state information... Done
wget is already the newest version (1.20.3-1ubuntu1).
software-properties-common is already the newest version (0.98.9.5).
apt-transport-https is already the newest version (2.0.6).
The following packages were automatically installed and are no longer required:
  linux-headers-5.11.0-27-generic linux-hwe-5.11-headers-5.11.0-27
  linux-image-5.11.0-27-generic linux-modules-5.11.0-27-generic
  linux-modules-extra-5.11.0-27-generic
Use 'sudo apt autoremove' to remove them.
0 to upgrade, 0 to newly install, 0 to remove and 15 not to upgrade.
pj@pj-Aspire-TC-780:~$ wget -q http://www.webmin.com/jcameron-key.asc -O- | sudo
 apt-key add -
OK
pj@pj-Aspire-TC-780:~$ sudo add-apt-repository "deb [arch=amd64] http:download.w
ebmin.com/download/repository sarge contrib"
```

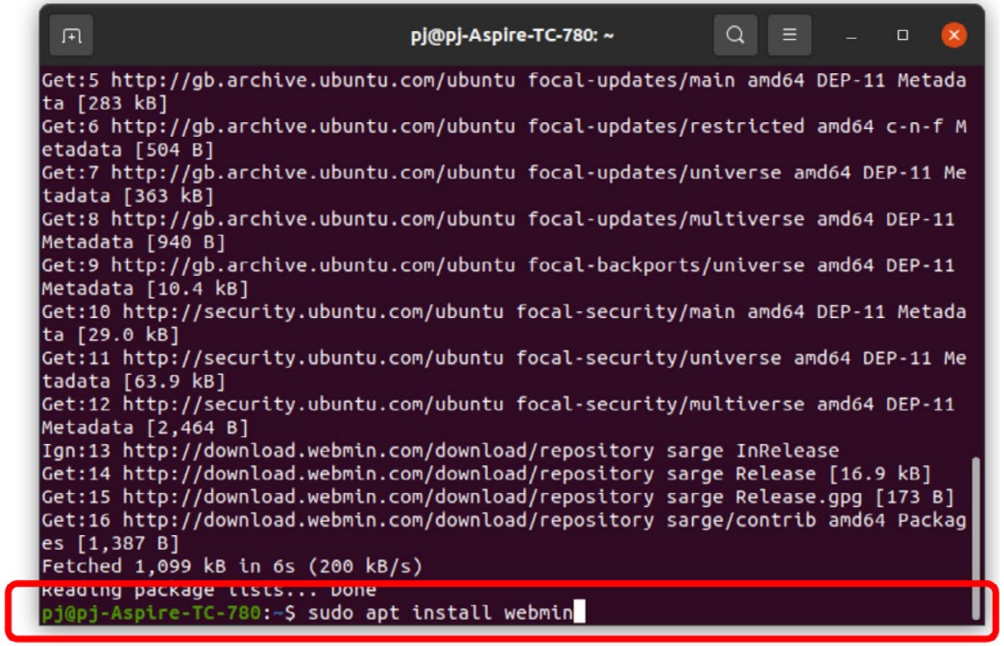


```
Get:5 http://gb.archive.ubuntu.com/ubuntu focal-updates/main amd64 DEP-11 Metada
ta [283 kB]
Get:6 http://gb.archive.ubuntu.com/ubuntu focal-updates/restricted amd64 c-n-f M
etadata [504 B]
Get:7 http://gb.archive.ubuntu.com/ubuntu focal-updates/universe amd64 DEP-11 Me
tadata [363 kB]
Get:8 http://gb.archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 DEP-11
Metadata [940 B]
Get:9 http://gb.archive.ubuntu.com/ubuntu focal-backports/universe amd64 DEP-11
Metadata [10.4 kB]
Get:10 http://security.ubuntu.com/ubuntu focal-security/main amd64 DEP-11 Metada
ta [29.0 kB]
Get:11 http://security.ubuntu.com/ubuntu focal-security/universe amd64 DEP-11 Me
tadata [63.9 kB]
Get:12 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 DEP-11
Metadata [2,464 B]
Ign:13 http://download.webmin.com/download/repository sarge InRelease
Get:14 http://download.webmin.com/download/repository sarge Release [16.9 kB]
Get:15 http://download.webmin.com/download/repository sarge Release.gpg [173 B]
Get:16 http://download.webmin.com/download/repository sarge/contrib amd64 Packag
es [1,387 B]
Fetched 1,099 kB in 6s (200 kB/s)
Reading package lists... Done
pj@pj-Aspire-TC-780:~$
```

Step 3

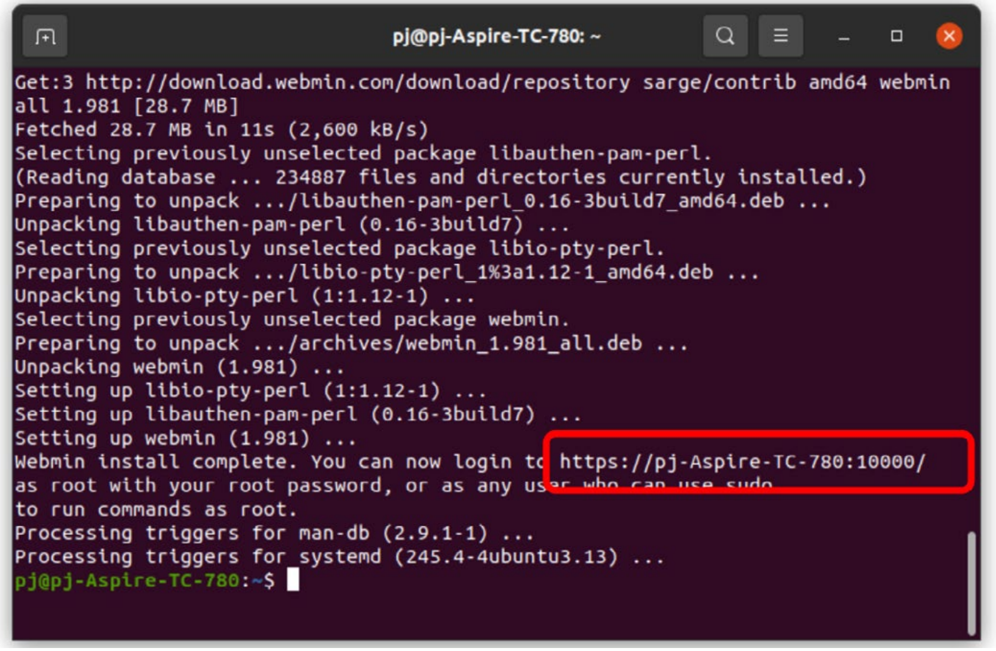
We can now install the latest version of Webmin.

```
sudo apt install webmin
```



```
Get:5 http://gb.archive.ubuntu.com/ubuntu focal-updates/main amd64 DEP-11 Metada
ta [283 kB]
Get:6 http://gb.archive.ubuntu.com/ubuntu focal-updates/restricted amd64 c-n-f M
etadata [504 B]
Get:7 http://gb.archive.ubuntu.com/ubuntu focal-updates/universe amd64 DEP-11 Me
tadata [363 kB]
Get:8 http://gb.archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 DEP-11
Metadata [940 B]
Get:9 http://gb.archive.ubuntu.com/ubuntu focal-backports/universe amd64 DEP-11
Metadata [10.4 kB]
Get:10 http://security.ubuntu.com/ubuntu focal-security/main amd64 DEP-11 Metada
ta [29.0 kB]
Get:11 http://security.ubuntu.com/ubuntu focal-security/universe amd64 DEP-11 Me
tadata [63.9 kB]
Get:12 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 DEP-11
Metadata [2,464 B]
Ign:13 http://download.webmin.com/download/repository sarge InRelease
Get:14 http://download.webmin.com/download/repository sarge Release [16.9 kB]
Get:15 http://download.webmin.com/download/repository sarge Release.gpg [173 B]
Get:16 http://download.webmin.com/download/repository sarge/contrib amd64 Packag
es [1,387 B]
Fetched 1,099 kB in 6s (200 kB/s)
Reading package lists... Done
pj@pj-Aspire-TC-780:~$ sudo apt install webmin
```

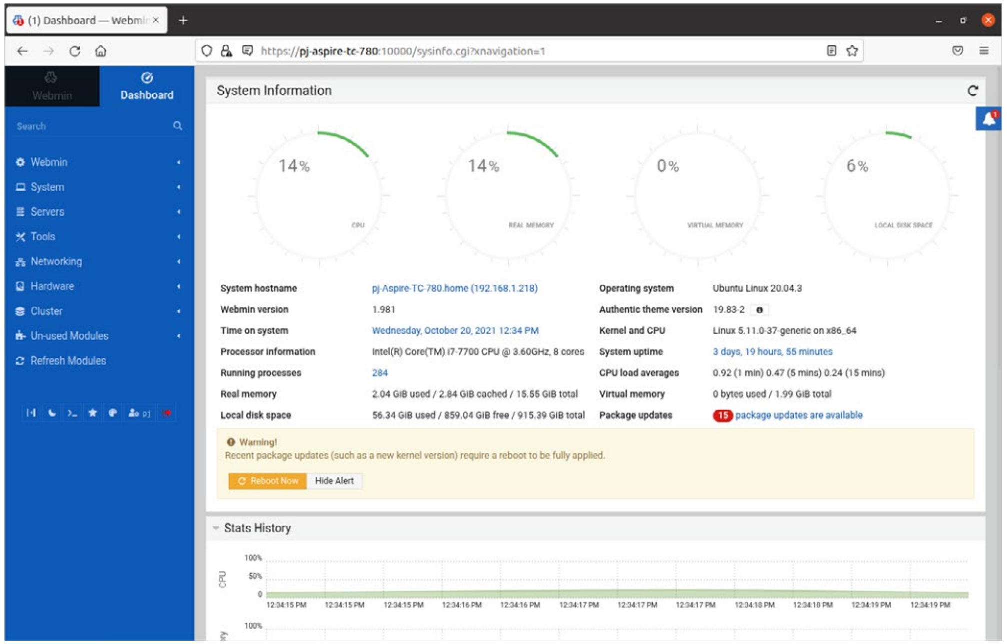
When the installation is complete you will see a similar output to the image below, the web address to access your personal Webmin dashboard will be in this last section. You then need to open a web browser and add this in as a URL. You may be prompted by a security message as it is not a standard web address to locate, click on advanced and allow the web browser to open the URL.



```
Get:3 http://download.webmin.com/download/repository sarge/contrib amd64 webmin
all 1.981 [28.7 MB]
Fetched 28.7 MB in 11s (2,600 kB/s)
Selecting previously unselected package libauthen-pam-perl.
(Reading database ... 234887 files and directories currently installed.)
Preparing to unpack .../libauthen-pam-perl_0.16-3build7_amd64.deb ...
Unpacking libauthen-pam-perl (0.16-3build7) ...
Selecting previously unselected package libio-pty-perl.
Preparing to unpack .../libio-pty-perl_1%3a1.12-1_amd64.deb ...
Unpacking libio-pty-perl (1:1.12-1) ...
Selecting previously unselected package webmin.
Preparing to unpack .../archives/webmin_1.981_all.deb ...
Unpacking webmin (1.981) ...
Setting up libio-pty-perl (1:1.12-1) ...
Setting up libauthen-pam-perl (0.16-3build7) ...
Setting up webmin (1.981) ...
Webmin install complete. You can now login to https://pj-Aspire-TC-780:10000/
as root with your root password, or as any user who can use sudo
to run commands as root.
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for systemd (245.4-4ubuntu3.13) ...
pj@pj-Aspire-TC-780:~$
```

You will be prompted with a login screen, and you need to use your user login details.

You will then be able to see the dashboard as below, with a range of options on the left relating to your server.



System hostname	pj-Aspire-TC-780.home (192.168.1.218)	Operating system	Ubuntu Linux 20.04.3
Webmin version	1.981	Authentic theme version	19.83-2
Time on system	Wednesday, October 20, 2021 12:34 PM	Kernel and CPU	Linux 5.11.0-37-generic on x86_64
Processor information	Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz, 8 cores	System uptime	3 days, 19 hours, 55 minutes
Running processes	284	CPU load averages	0.92 (1 min) 0.47 (5 mins) 0.24 (15 mins)
Real memory	2.04 GiB used / 2.84 GiB cached / 15.55 GiB total	Virtual memory	0 bytes used / 1.99 GiB total
Local disk space	56.34 GiB used / 859.04 GiB free / 915.39 GiB total	Package updates	15 package updates are available

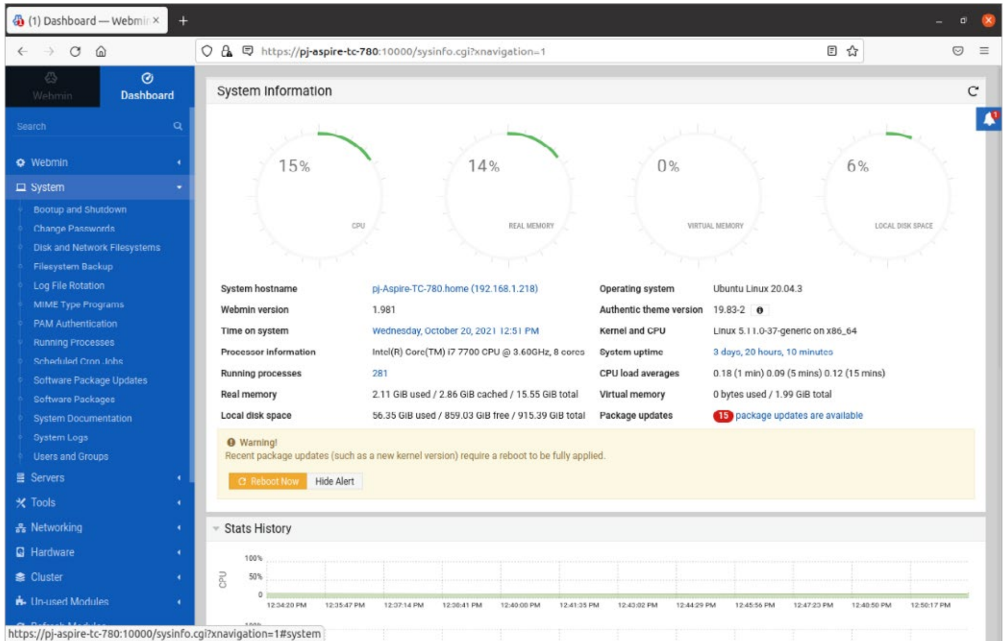
Warning!
Recent package updates (such as a new kernel version) require a reboot to be fully applied.

Using Webmin

There are lots of options on the left-hand side of the dashboard

- Webmin
- System
- Servers
- Tools
- Networking
- Hardware
- Cluster
- Unused Modules
- Refresh Modules

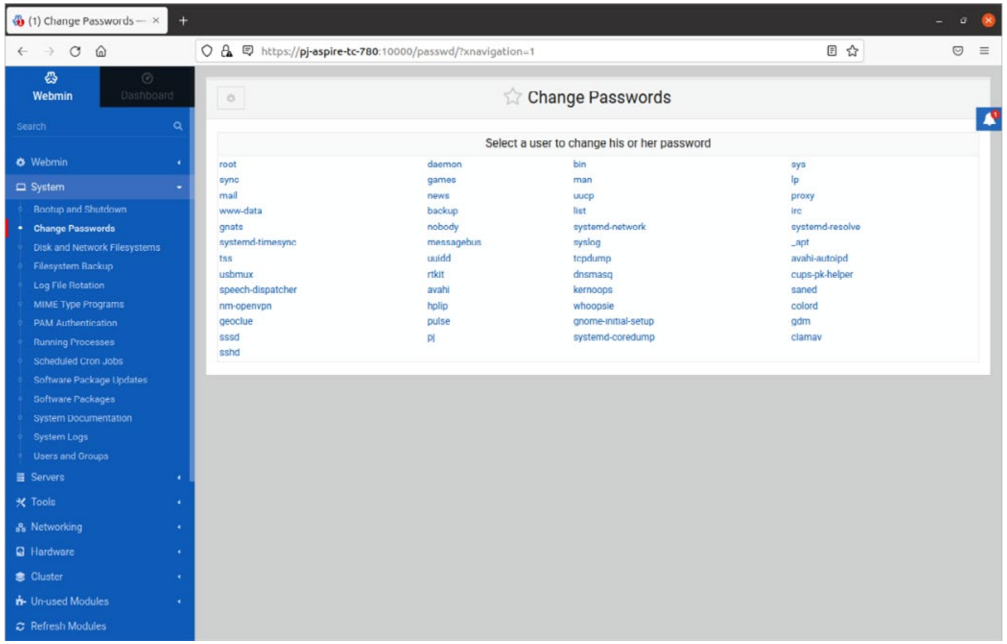
Each of these areas have a drop-down menu that can be visible when you click on the arrow next to the area name.



System hostname	pj-Aspire-TC-780.home (192.168.1.218)	Operating system	Ubuntu Linux 20.04.3
Webmin version	1.981	Authentic theme version	19.83-2
Time on system	Wednesday, October 20, 2021 12:51 PM	Kernel and CPU	Linux 5.11.0-37-generic on x86_64
Processor information	Intel(R) Core(TM) i7 7700 CPU @ 3.60GHz, 8 cores	System uptime	3 days, 20 hours, 10 minutes
Running processes	281	CPU load averages	0.18 (1 min) 0.09 (5 mins) 0.12 (15 mins)
Real memory	2.11 GiB used / 2.86 GiB cached / 15.55 GiB total	Virtual memory	0 bytes used / 1.99 GiB total
Local disk space	56.35 GiB used / 859.03 GiB free / 915.39 GiB total	Package updates	15 package updates are available

Warning!
Recent package updates (such as a new kernel version) require a reboot to be fully applied.

Under **System** we can change passwords by selecting the user and editing the details stored.

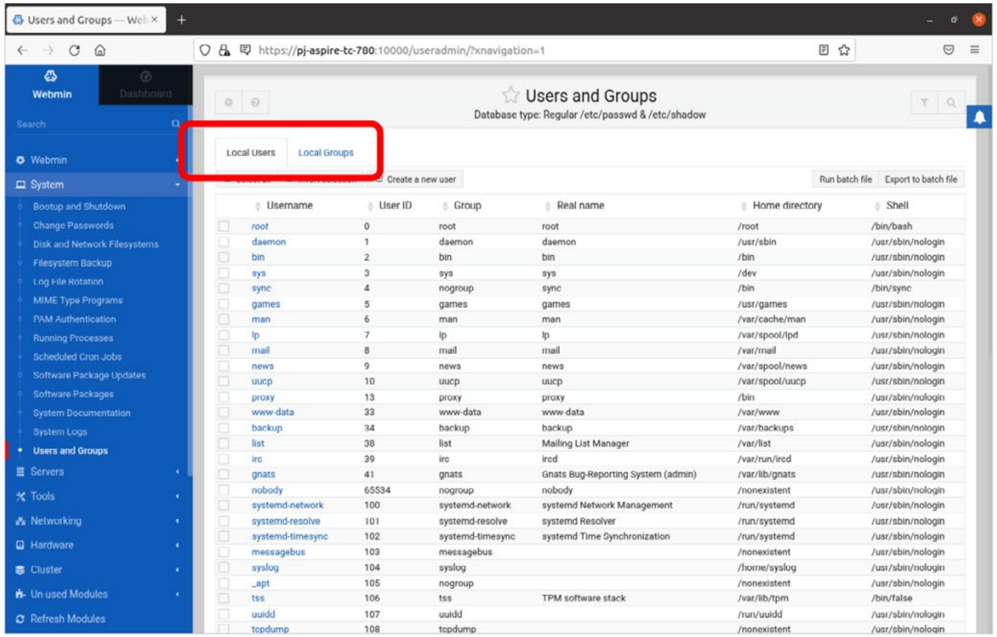


Change Passwords

Select a user to change his or her password

root	daemon	bin	sys
sync	games	man	lp
mail	news	uucp	proxy
www-data	backup	list	irc
gnats	nobody	systemd-network	systemd-resolve
systemd-timesync	messagebus	syslog	_apt
tss	uuidd	tcpdump	avahi-autoipd
usbmux	rtkit	dnsmasq	cups-pk-helper
speech-dispatcher	avahi	kernoops	saned
nm-openvpn	hplip	whoopsie	colord
geoclue	pulse	gnome-initial-setup	gdm
sssd	pj	systemd-coredump	clamav
sshd			

Under **System** we can also view all the users and groups that are set up on the system and edit any details here too. There are two tabs to move between the users and groups set up.

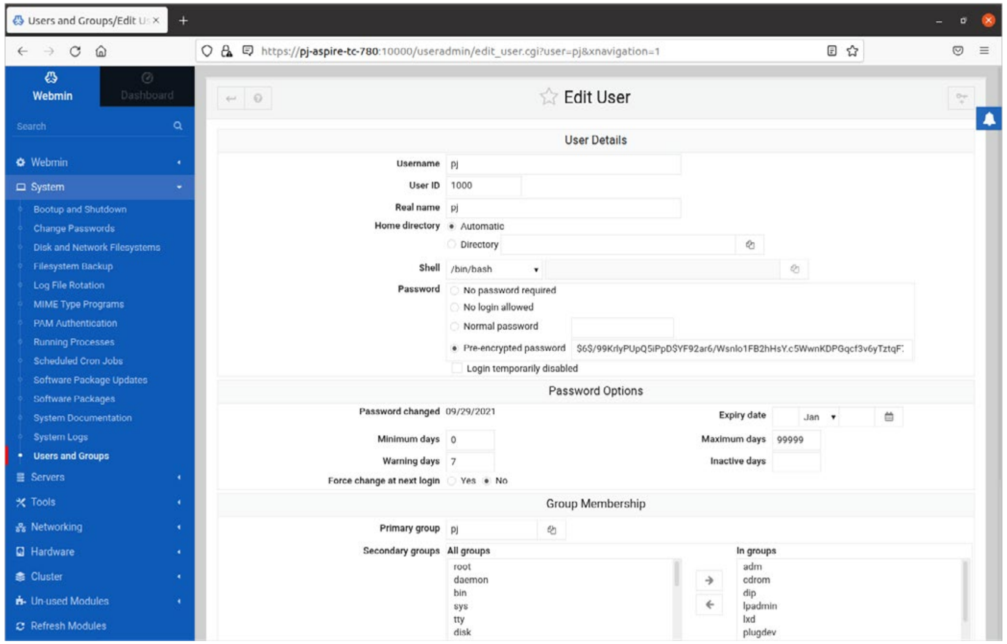


Users and Groups

Database type: Regular /etc/passwd & /etc/shadow

	Username	User ID	Group	Real name	Home directory	Shell
□	root	0	root	root	/root	/bin/bash
□	daemon	1	daemon	daemon	/usr/sbin	/usr/sbin/nologin
□	bin	2	bin	bin	/bin	/usr/sbin/nologin
□	sys	3	sys	sys	/dev	/usr/sbin/nologin
□	sync	4	nogroup	sync	/bin	/bin/sync
□	games	5	games	games	/usr/games	/usr/sbin/nologin
□	man	6	man	man	/var/cache/man	/usr/sbin/nologin
□	lp	7	lp	lp	/var/spool/lpd	/usr/sbin/nologin
□	mail	8	mail	mail	/var/mail	/usr/sbin/nologin
□	news	9	news	news	/var/spool/news	/usr/sbin/nologin
□	uucp	10	uucp	uucp	/var/spool/uucp	/usr/sbin/nologin
□	proxy	13	proxy	proxy	/bin	/usr/sbin/nologin
□	www-data	33	www-data	www-data	/var/www	/usr/sbin/nologin
□	backup	34	backup	backup	/var/backups	/usr/sbin/nologin
□	list	38	list	Mailing List Manager	/var/list	/usr/sbin/nologin
□	irc	39	irc	ircd	/var/run/ircd	/usr/sbin/nologin
□	gnats	41	gnats	Gnats Bug-Reporting System (admin)	/var/lib/gnats	/usr/sbin/nologin
□	nobody	65534	nogroup	nobody	/nonexistent	/usr/sbin/nologin
□	systemd-network	100	systemd-network	systemd Network Management	/run/systemd	/usr/sbin/nologin
□	systemd-resolve	101	systemd-resolve	systemd Resolver	/run/systemd	/usr/sbin/nologin
□	systemd-timesync	102	systemd-timesync	systemd Time Synchronization	/run/systemd	/usr/sbin/nologin
□	messagebus	103	messagebus		/nonexistent	/usr/sbin/nologin
□	syslog	104	syslog		/home/syslog	/usr/sbin/nologin
□	_apt	105	nogroup		/nonexistent	/usr/sbin/nologin
□	tss	106	tss	TPM software stack	/var/lib/tpm	/bin/false
□	uuidd	107	uuidd		/run/uuidd	/usr/sbin/nologin
□	tcpdump	108	tcpdump		/nonexistent	/usr/sbin/nologin

When you click on a user you can see the information relating to the user and edit any details as well as what groups they are linked with.



Edit User

User Details

Username	pj
User ID	1000
Real name	pj
Home directory	● Automatic ○ Directory
Shell	/bin/bash
Password	○ No password required ○ No login allowed ○ Normal password ● Pre-encrypted password $6$/99KrlyPUpQ5iPpD$YF92ar6/Wsnlo1FB2hHsY.c5WwnKDPGqcf3v6yTztqF □ Login temporarily disabled

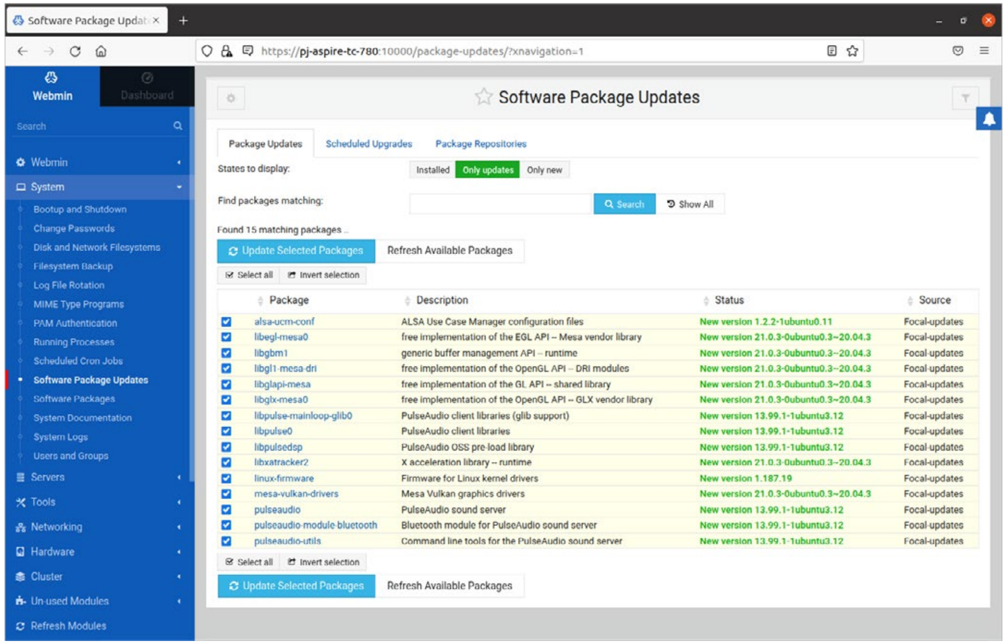
Password Options

Password changed	09/29/2021	Expiry date	Jan
Minimum days	0	Maximum days	99999
Warning days	7	Inactive days	
Force change at next login	○ Yes ● No		

Group Membership

Primary group	pj	
Secondary groups	All groups	In groups
	root daemon bin sys tty disk	adm cdrom dip lpadmin lxd plugdev

Under **System** we can check for software updates and install any of the selected updates.



Software Package Updates

Package Updates | Scheduled Upgrades | Package Repositories

States to display: Installed | Only updates | Only new

Find packages matching: Search | Show All

Found 15 matching packages ..

Update Selected Packages | Refresh Available Packages

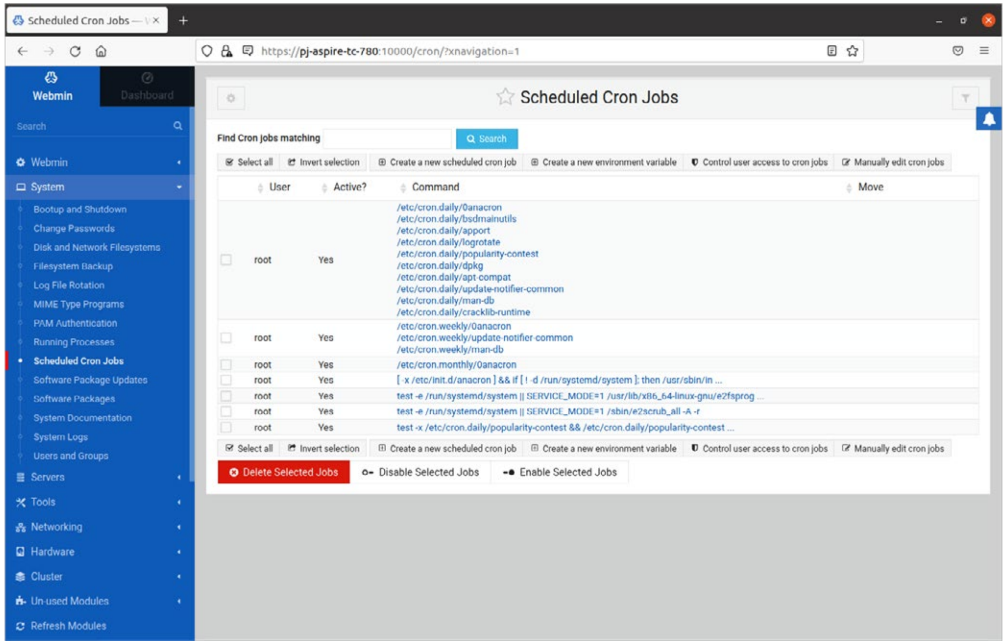
Select all | Invert selection

	Package	Description	Status	Source
☑	alsa-ucm-conf	ALSA Use Case Manager configuration files	New version 1.2.2-1ubuntu0.11	Focal-updates
☑	libegl-mesa0	free implementation of the EGL API -- Mesa vendor library	New version 21.0.3-0ubuntu0.3~20.04.3	Focal-updates
☑	libgbm1	generic buffer management API -- runtime	New version 21.0.3-0ubuntu0.3~20.04.3	Focal-updates
☑	libgl1-mesa-dri	free implementation of the OpenGL API -- DRI modules	New version 21.0.3-0ubuntu0.3~20.04.3	Focal-updates
☑	libglapi-mesa	free implementation of the GL API -- shared library	New version 21.0.3-0ubuntu0.3~20.04.3	Focal-updates
☑	libglx-mesa0	free implementation of the OpenGL API -- GLX vendor library	New version 21.0.3-0ubuntu0.3~20.04.3	Focal-updates
☑	libpulse-mainloop-glib0	PulseAudio client libraries (glib support)	New version 13.99.1-1ubuntu3.12	Focal-updates
☑	libpulse0	PulseAudio client libraries	New version 13.99.1-1ubuntu3.12	Focal-updates
☑	libpulsedsp	PulseAudio OSS pre-load library	New version 13.99.1-1ubuntu3.12	Focal-updates
☑	libxatracker2	X acceleration library -- runtime	New version 21.0.3-0ubuntu0.3~20.04.3	Focal-updates
☑	linux-firmware	Firmware for Linux kernel drivers	New version 1.187.19	Focal-updates
☑	mesa-vulkan-drivers	Mesa Vulkan graphics drivers	New version 21.0.3-0ubuntu0.3~20.04.3	Focal-updates
☑	pulseaudio	PulseAudio sound server	New version 13.99.1-1ubuntu3.12	Focal-updates
☑	pulseaudio-module-bluetooth	Bluetooth module for PulseAudio sound server	New version 13.99.1-1ubuntu3.12	Focal-updates
☑	pulseaudio-utils	Command line tools for the PulseAudio sound server	New version 13.99.1-1ubuntu3.12	Focal-updates

Select all | Invert selection

Update Selected Packages | Refresh Available Packages

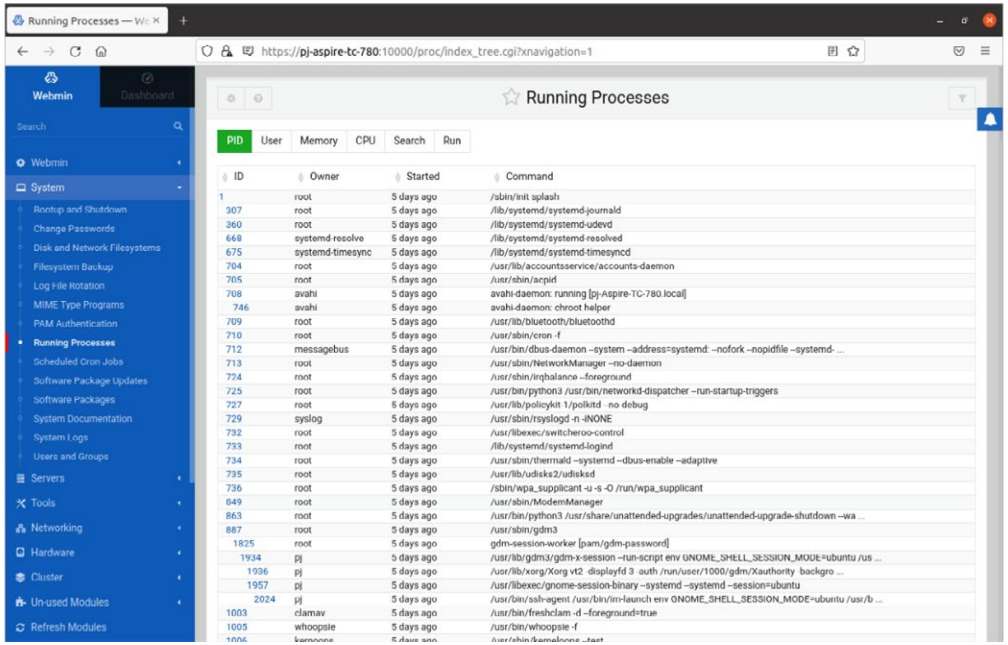
Under **`System`** we can also see the scheduled cron jobs. Cron jobs are run periodically at fixed times, date, or intervals.



Scheduled Cron Jobs

	User	Active?	Command	Move
□	root	Yes	/etc/cron.daily/0anacron /etc/cron.daily/bsdmainutils /etc/cron.daily/apport /etc/cron.daily/logrotate /etc/cron.daily/popularity-contest /etc/cron.daily/dpkg /etc/cron.daily/apt-compat /etc/cron.daily/update-notifier-common /etc/cron.daily/man-db /etc/cron.daily/cracklib-runtime	
□	root	Yes	/etc/cron.weekly/0anacron /etc/cron.weekly/update-notifier-common /etc/cron.weekly/man-db	
□	root	Yes	/etc/cron.monthly/0anacron	
□	root	Yes	[-x /etc/init.d/anacron] && if [! -d /run/systemd/system]; then /usr/sbin/in ...	
□	root	Yes	test -e /run/systemd/system || SERVICE_MODE=1 /usr/lib/x86_64-linux-gnu/e2fsprog ...	
□	root	Yes	test -e /run/systemd/system || SERVICE_MODE=1 /sbin/e2scrub_all -A -r	
□	root	Yes	test -x /etc/cron.daily/popularity-contest && /etc/cron.daily/popularity-contest ...	

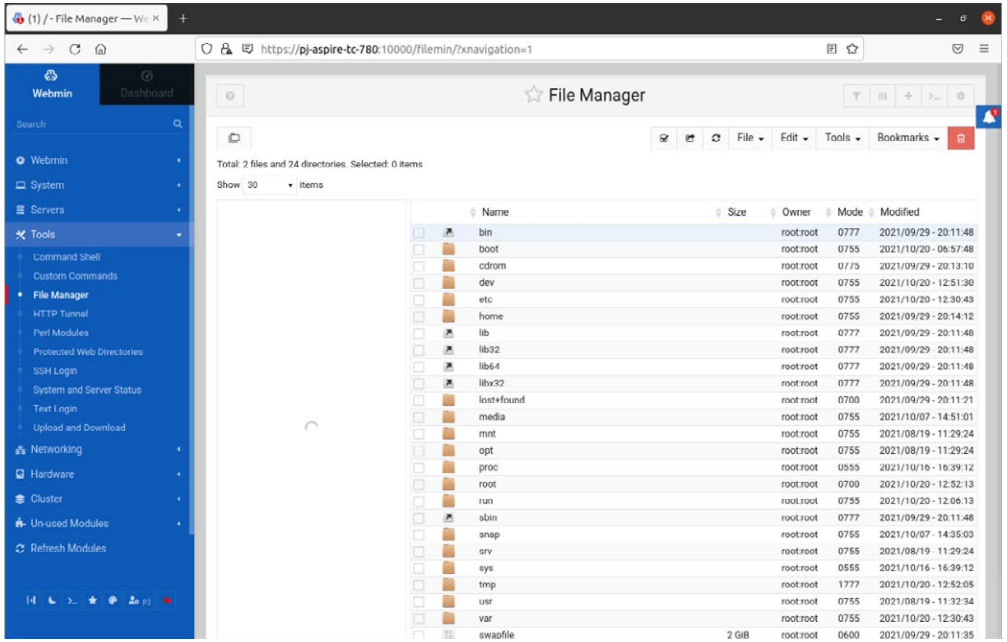
Under **`System`** we can also check the processes that are running and use this to see if anything that should not be there or running needs to be stopped.



Running Processes

ID	Owner	Started	Command
1	root	5 days ago	/sbin/init splash
307	root	5 days ago	/lib/systemd/systemd-journald
360	root	5 days ago	/lib/systemd/systemd-udevd
668	systemd-resolve	5 days ago	/lib/systemd/systemd-resolved
675	systemd-timesync	5 days ago	/lib/systemd/systemd-timesyncd
704	root	5 days ago	/usr/lib/accountsservice/accounts-daemon
705	root	5 days ago	/usr/sbin/acpid
708	avahi	5 days ago	avahi-daemon: running [pj-Aspire-TC-780.local]
746	avahi	5 days ago	avahi-daemon: chroot helper
709	root	5 days ago	/usr/lib/bluetooth/bluetoothd
710	root	5 days ago	/usr/sbin/cron -f
712	messagebus	5 days ago	/usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd- ...
713	root	5 days ago	/usr/sbin/NetworkManager --no-daemon
724	root	5 days ago	/usr/sbin/irqbalance --foreground
725	root	5 days ago	/usr/bin/python3 /usr/bin/networkd-dispatcher --run-startup-triggers
727	root	5 days ago	/usr/lib/policykit-1/polkitd --no-debug
729	syslog	5 days ago	/usr/sbin/rsyslogd -n -iNONE
732	root	5 days ago	/usr/libexec/switcheroo-control
733	root	5 days ago	/lib/systemd/systemd-logind
734	root	5 days ago	/usr/sbin/thermald --systemd --dbus-enable --adaptive
735	root	5 days ago	/usr/lib/udisks2/udisksd
736	root	5 days ago	/sbin/wpa_supplicant -u -s -O /run/wpa_supplicant
849	root	5 days ago	/usr/sbin/ModemManager
863	root	5 days ago	/usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown --wa ...
887	root	5 days ago	/usr/sbin/gdm3
1825	root	5 days ago	gdm-session-worker [pam/gdm-password]
1934	pj	5 days ago	/usr/lib/gdm3/gdm-x-session --run-script env GNOME_SHELL_SESSION_MODE=ubuntu /us ...
1936	pj	5 days ago	/usr/lib/xorg/Xorg vt2 -displayfd 3 -auth /run/user/1000/gdm/Xauthority -backgro ...
1957	pj	5 days ago	/usr/libexec/gnome-session-binary --systemd --systemd --session=ubuntu
2024	pj	5 days ago	/usr/bin/ssh-agent /usr/bin/im-launch env GNOME_SHELL_SESSION_MODE=ubuntu /usr/b ...
1003	clamav	5 days ago	/usr/bin/freshclam -d --foreground=true
1005	whoopsie	5 days ago	/usr/bin/whoopsie -f
1006	kernoops	5 days ago	/usr/sbin/kerneloops --test

There are other areas to look at too, you can open the file manager under **Tools** to see all that is stored on the system.



Total: 2 files and 24 directories. Selected: 0 items

Show 30 items

Name	Size	Owner	Mode	Modified
bin		root:root	0777	2021/09/29 - 20:11:48
boot		root:root	0755	2021/10/20 - 06:57:48
cdrom		root:root	0775	2021/09/29 - 20:13:10
dev		root:root	0755	2021/10/20 - 12:51:30
etc		root:root	0755	2021/10/20 - 12:30:43
home		root:root	0755	2021/09/29 - 20:14:12
lib		root:root	0777	2021/09/29 - 20:11:48
lib32		root:root	0777	2021/09/29 - 20:11:48
lib64		root:root	0777	2021/09/29 - 20:11:48
libx32		root:root	0777	2021/09/29 - 20:11:48
lost+found		root:root	0700	2021/09/29 - 20:11:21
media		root:root	0755	2021/10/07 - 14:51:01
mnt		root:root	0755	2021/08/19 - 11:29:24
opt		root:root	0755	2021/08/19 - 11:29:24
proc		root:root	0555	2021/10/16 - 16:39:12
root		root:root	0700	2021/10/20 - 12:52:13
run		root:root	0755	2021/10/20 - 12:06:13
sbin		root:root	0777	2021/09/29 - 20:11:48
snap		root:root	0755	2021/10/07 - 14:35:03
srv		root:root	0755	2021/08/19 - 11:29:24
sys		root:root	0555	2021/10/16 - 16:39:12
tmp		root:root	1777	2021/10/20 - 12:52:05
usr		root:root	0755	2021/08/19 - 11:32:34
var		root:root	0755	2021/10/20 - 12:30:43
swapfile	2 GiB	root:root	0600	2021/09/29 - 20:11:35

There is a lot under this application, and it is worth looking at each area to see how it can be used to help secure your device and maintain the functionality of the system further.

Cyber-Security Fact:
Consider carefully who you give access to this to, any user on this application could edit, add, delete anything that is essential to the running of the system as well as give access to others to use the system without your knowledge.