لَا يُؤْمِنُ أَحَدُكُمْ، حتَّى يُحِبَّ لأخِيهِ ما يُحِبُّ لِنَفْسِهِ.

LINUX ESSENTIALS

بِسْمِ اللهِ الرَّحْمنِ الرَّحِيمِ

وَمَن يَتَّقِ اللَّهَ يَجْعَل لَّهُ مَخْرَجًا (2)وَيَرْزُقْهُ مِنْ حَيْثُ لَا يَحْتَسِبُ ۚ وَمَن يَتَوَكَّلْ عَلَى اللَّهِ فَهُوَ حَسْبُهُ ۚ إِنَّ اللَّهَ بَالِغُ أَمْرِهِ ۚ قَدْ جَعَلَ اللَّهُ لِكُلِّ شَيْءٍ قَدْرًا (3)سورة الطلاق

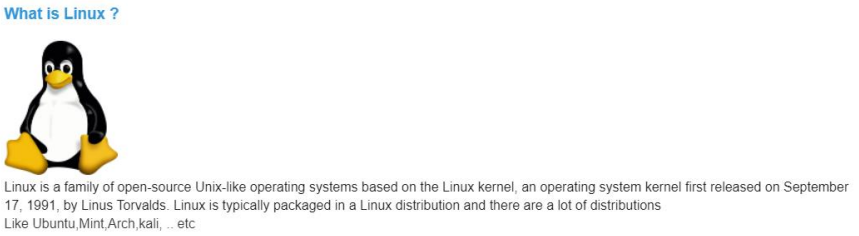
CyberTalents Course

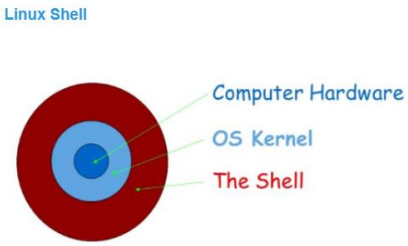
By : Eng Mohamed Ewies

لَا يُؤْمِنُ أَحَدُكُمْ، حتَّى يُحِبَّ لأخِيهِ ما يُحِبُّ لِنَفْسِهِ.

What is SSH?

1.The Secure Shell Protocol (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network.





Typical applications include remote command-line, login, and remote command execution, but any network service can be secured with SSH

2.SSH is running by default on port 22 but it is not always the case.

3.There are several ways to connect to a system with SSH like PuTTY App or from your linux terminal.

What is Putty?

PuTTY is a free and open-source terminal emulator, serial console, and network file transfer application.

It supports several network protocols, including SCP, SSH, Telnet, rlogin, and raw socket connection.

---

can also connect with the command line at your terminal

All you have to do is open the terminal window and type this command :

$ ssh username@ip_address -p port_number

Username: the username that you want to login with.

Ip_address: the ip of the remote machine اللي هنتصل بيها مش جهازنا احنا ركز يبيه :)

-p port_number: you don't have to type this if it is running on port 22

---

pwd → One of the easiest built-in Linux commands to remember as it stands for `print working directory`

Uname -a → This command prints out your Operating system's kernel version and Architecture

hostname → This command prints out your machine's hostname (Generally defined in /etc/hosts)

لَا يُؤْمِنُ أَحَدُكُمْ، حتَّى يُحِبَّ لأخِيهِ ما يُحِبُّ لِنَفْسِهِ.

id → This command prints out your UID , GID, and also all the groups that your current user is in.

System information commands:

whoami → This command prints out your current user

'echo' is similar to print. It will print out the arguments passed to it whether it's a variable or text

In the Linux terminal, the strings that start with a dollar sign ($) are variables just like in PHP.

Linux has many pre-defined variables that can be used anywhere on the system!

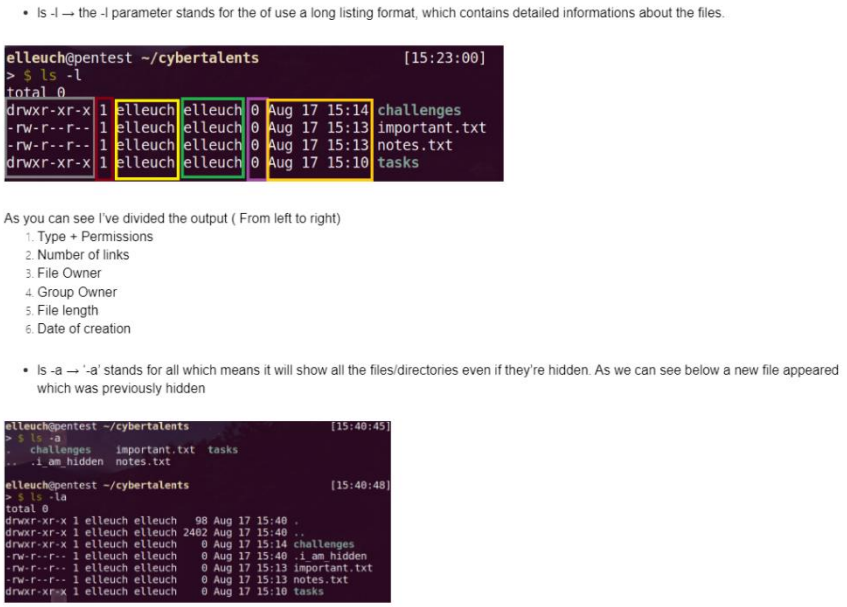
In our case, the pre-defined variable 'PWD' لازم تبقى كلها حروف كبيره مش صغيره contains the current working directory

ls → This is also a built-in command in Linux, which is the abbreviation of 'list' it basically lists all the files/directories on your current working directory. As shown in the picture below, we can even differentiate between files and directories (The colours differs from distro to distro and also can be changed manually from the settings)

ls -l → the -l parameter stands for the of use a long listing format, which contains detailed information about the files.

ls -a → '-a' stands for all which means it will show all the files/directories even if they're hidden.

As we can see below a new file appeared which was previously hidden



We will be using the 'man' command. It will display to us the whole documentation of the certain command

how to navigate in the system. We'll be using the built-in command 'cd'

So what if we want to go back to the cybertalents's folder?

→ We can use double dots to do it

لَا يُؤْمِنُ أَحَدُكُمْ، حتَّى يُحِبَّ لأخِيهِ ما يُحِبُّ لِنَفْسِهِ.

What if we want to go back to /home/elleuch/cybertalents/tasks which were our previous working directory type cd -

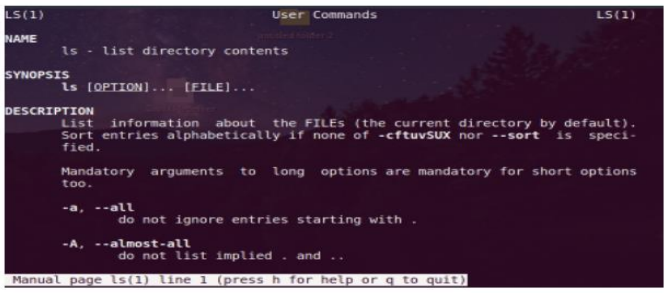
mkdir → With this built-in command we can create directories

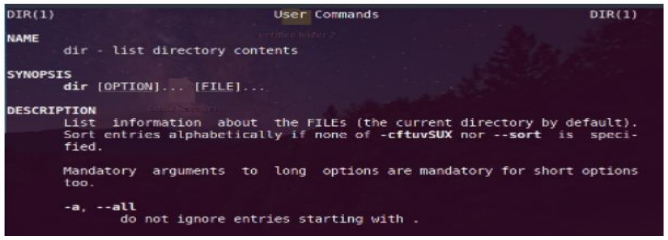
touch → With this built-in command we can create files

mv → With this built-in command we can either move or rename files and directories.

It can happen, even to the best of us, that sometimes we forget the syntax of certain commands. But likely Linux has its built-in manual as well to guide us.

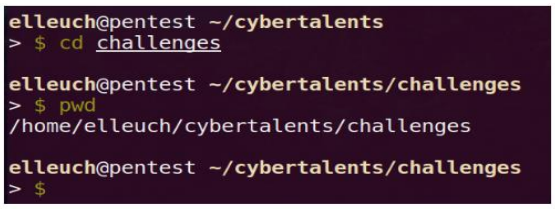
- We will be using the 'man' command. It will display to us the whole documentation of the certain command. Let's try it. Pretty handy command to use when needed



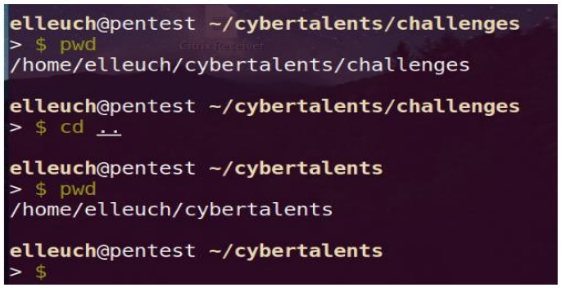


Since now we have learned how to list directories files and how to know our current working directory. Let's now learn how to navigate in the system. We'll be using the built-in command 'cd'
From previous screenshots, we can see that have 2 directories challenges and tasks.

- Let's try to move to one of them.



- So what if we want to go back to the cybertalents's folder?
  → We can use double dots to do it



لَا يُؤْمِنُ أَحَدُكُمْ، حتَّى يُحِبَّ لأخِيهِ ما يُحِبُّ لِنَفْسِهِ.

- Another trick to know, In Linux '~' is an alias to /home/<youruser>. This means we can cd into our home directory with ease

```
elleuch@pentest ~/cybertalents/tasks
> $ cd ~

elleuch@pentest ~
> $ pwd
/home/elleuch
```

```
elleuch@pentest ~/cybertalents/tasks
> $ echo ~
/home/elleuch
```

- What if we wanna go back to /home/elleuch/cybertalents/tasks which were our previous working directory

```
elleuch@pentest ~
> $ pwd
/home/elleuch

elleuch@pentest ~
> $ cd -
~/cybertalents/tasks

elleuch@pentest ~/cybertalents/tasks
> $ pwd
/home/elleuch/cybertalents/tasks
```

- mkdir → With this built-in command we can create directories.

```
> $ ls

elleuch@pentest ~/cybertalents/challenges
> $ mkdir web

elleuch@pentest ~/cybertalents/challenges
> $ ls
web
```

- touch → With this built-in command we can create files

```
elleuch@pentest ~/cybertalents/challenges
> $ touch hard_challenge.md

elleuch@pentest ~/cybertalents/challenges
> $ ls
hard_challenge.md  web
```

- mv → With this built-in command we can either move or rename files and directories. Let's try to move the hard_challenge.md from the challenges directory to the tasks directory then rename it to web.md

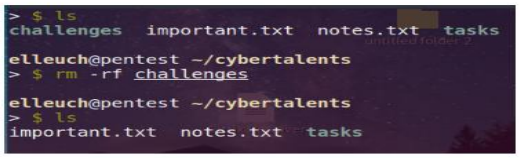
```
> $ pwd
/home/elleuch/cybertalents/tasks

elleuch@pentest ~/cybertalents/tasks
> $ mv ../challenges/hard_challenge.md .

elleuch@pentest ~/cybertalents/tasks
> $ ls
hard_challenge.md
```

مَن أَحْدَثَ في أَمْرِنَا هذا ما ليسَ فِيهِ، فَهو رَدٌّ

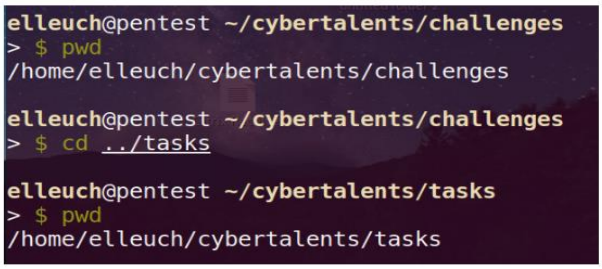
وَمَا خَلَقْتُ الْجِنَّ وَالْإِنسَ إِلَّا لِيَعْبُدُونِ

لَا يُؤْمِنُ أَحَدُكُمْ، حتَّى يُحِبَّ لأخِيهِ ما يُحِبُّ لِنَفْسِهِ.

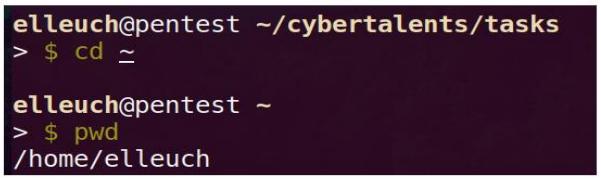
- rm → to remove files / rm -rf → to remove directories



- Another question, What if we want to change the tasks directory from the challenge directory? → We can also use the double dots



- Another trick to know, In Linux '~' is an alias to /home/<youruser>. This means we can cd into our home directory with ease



- What if we wanna go back to /home/elleuch/cybertalents/tasks which were our previous working directory

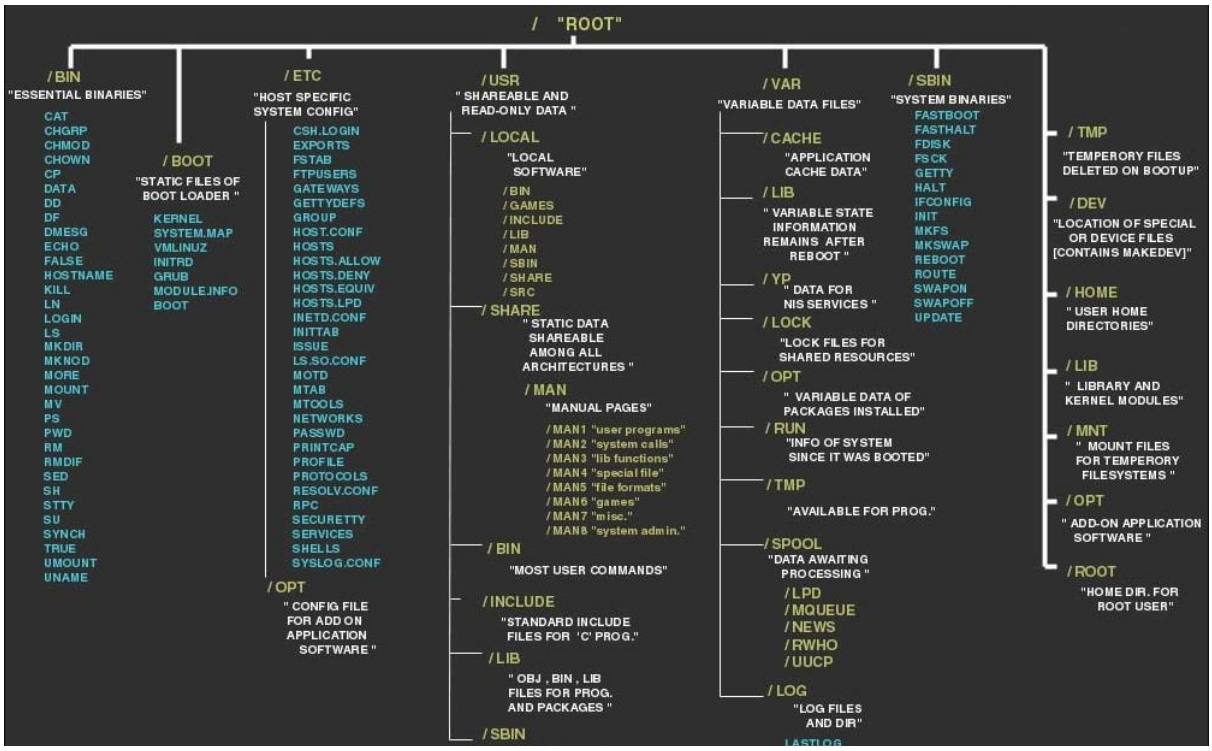
يَا أَيُّهَا النَّاسُ اعْبُدُوا رَبَّكُمْ الَّذِي خَلَقَكُمْ وَالَّذِينَ مِنْ قَبْلِكُمْ لَعَلَّكُمْ تَتَّقُونَ

أَلَمْ يَأْنِ لِلَّذِينَ آمَنُوا أَن تَخْشَعَ قُلُوبُهُمْ لِذِكْرِ اللَّهِ وَمَا نَزَلَ مِنَ الْحَقِّ وَلَا يَكُونُوا كَالَّذِينَ أُوتُوا الْكِتَابَ مِن قَبْلُ فَطَالَ عَلَيْهِمُ الْأَمَدُ فَقَسَتْ قُلُوبُهُمْ ۖ وَكَثِيرٌ مِّنْهُمْ فَاسِقُونَ

وَمَا خَلَقْتُ الْجِنَّ وَالْإِنسَ إِلَّا لِيَعْبُدُونِ

لَا يُؤْمِنُ أَحَدُكُمْ، حتَّى يُحِبَّ لأخِيهِ ما يُحِبُّ لِنَفْسِهِ.

Structure of Linux file system



/ ,This is the root directory which should contain only the directories needed at the top level of the file structure.

/bin , This is where the executable files are located. These files are available to all users.

/dev ,These are device drivers.

/etc , Supervisor directory commands, configuration files, disk configuration files, valid user lists, groups, ethernet, hosts, where to send critical messages.

/lib , Contains shared library files and sometimes other kernel-related files.

/home ,Contains the home directory for users and other accounts.

/tmp , Holds temporary files used between system boots.

/kernel , Contains kernel files.

/mnt , Used to mount other temporary file systems, such as cdrom and floppy for the CD-ROM drive and floppy diskette drive, respectively

وَمَا خَلَقْتُ الْجِنَّ وَالْإِنسَ إِلَّا لِيَعْبُدُونِ

لَا يُؤْمِنُ أَحَدُكُمْ، حتَّى يُحِبَّ لأخِيهِ ما يُحِبُّ لِنَفْسِهِ.

Software Installations with Terminal

apt-get command

apt-get is a command-line tool that helps in handling packages in Linux. Its main task is to retrieve the information and packages from the authenticated sources for installation, upgrade, and removal of packages along with their dependencies.

Here APT stands for the Advanced Packaging Tool.

To install a package we can use the command `sudo apt-get install package name`.

To remove a package we can use the command `sudo apt-get remove package name`.

To update the package database we can use the command `sudo apt-get update`.

To update all the packages to their latest version, we can use the command `sudo apt-get upgrade`.

Basic file operations :

Touch Command :

Touch is used to create a file.

Cat Command :

Cat is used to display file content, but the file is longer than the size of the window, so it scrolls past making it unreadable.

More Command :

More is used to display file content, but the file is longer than the size of the window, it will display one page at a time.

:) يعني التاني بيعمل عمل الاولاني بس على كبير

Head and Tail Commands :

Both tools are file operators to display a specific part of the file, Head command is used to display the first part of the file and Tail is the opposite; it displays the last part of the file.

Grep Command:

Grep is used to search for a keyword or a specific pattern in the file.

ex : $cat lines.txt | grep 77

line 77

|-->shift+\ 'back slash' (near to enter not that near NumLock)

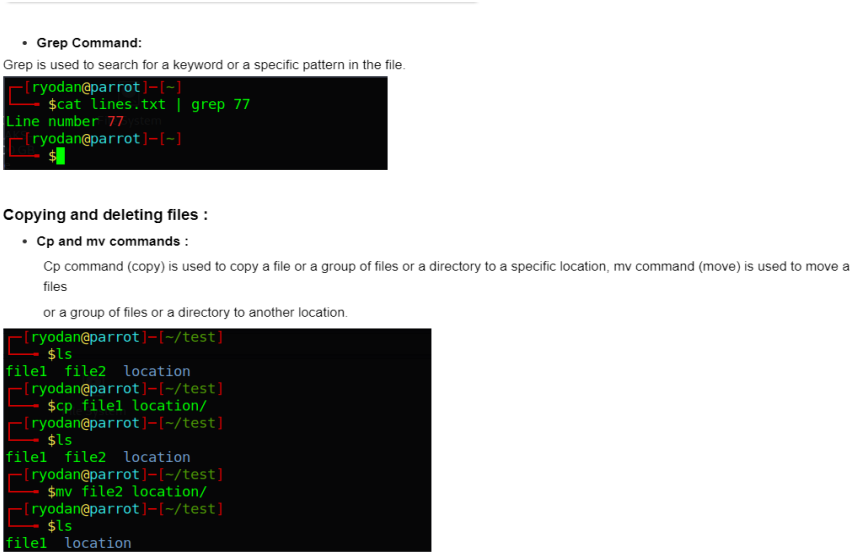
لَا يُؤْمِنُ أَحَدُكُمْ، حتَّى يُحِبَّ لأخِيهِ ما يُحِبُّ لِنَفْسِهِ.

Copying and deleting files :

Cp and mv commands :

Cp command (copy) is used to copy a file or a group of files or a directory to a specific location, mv command (move) is used to move a files

or a group of files or a directory to another location.



Wc Command :

Wc command is used to count the number of words, lines, and characters.

معلومه خطشيره :)

rm ~/Desktop/secret

secret معناها مسحت الملف

بس كتبتله عنوانه ازاي يروحله و ده تقدر تعمله مع اي ملف عموما ده كان ملف مش

directory

لإزاله دايريكتوري انت بكل بساطه هتزود

-rf

و لاحظ نفس الفكره هتقدر تطبقها مع اي امر

لو عايز افتح ملف

m.txt

و ده جوه ملف اسمه

hi

و ده على ال

desktop

هتكتب

cat ~/Desktop/hi/m.txt>>>>>>>>>>>>>>>file path مسار الملف

و بس كده استمتع 😊 و لاحظ لازم تحط ~

وَمَا خَلَقْتُ الْجِنَّ وَالْإِنسَ إِلَّا لِيَعْبُدُونِ

لَا يُؤْمِنُ أَحَدُكُمْ، حتَّى يُحِبَّ لأخِيهِ ما يُحِبُّ لِنَفْسِهِ.

What is the Linux command line?

The Linux command line is a text interface to the computer that is often referred to as the shell, terminal, console, prompt and other names.

The command line is a computer program intended to interpret commands. So, basically, a shell is a program that receives commands from the user and gives it to the OS to process, and it shows the output.

to open it press the key combination Ctrl+Alt+T in Ubuntu or from desktop menu option Terminal.

What is Text Manipulation?

Text manipulation is the process of using computer automation to modify text files on a large scale to suit the needs of the user.

An example of this can include changing the first character of every word in a text document to uppercase or changing every instance of a misspelled word throughout an entire document, to the correct spelling.

Also, consider the example below:

Cybertalents: This is the first char uppercase

CYBERTALENTS: This is all uppercase

CyBeRtAlEnTs: This is alternate-uppercase

cYbErTaLeNtS: This is alternate-lowercase

Text manipulation tools:

Sort

tr

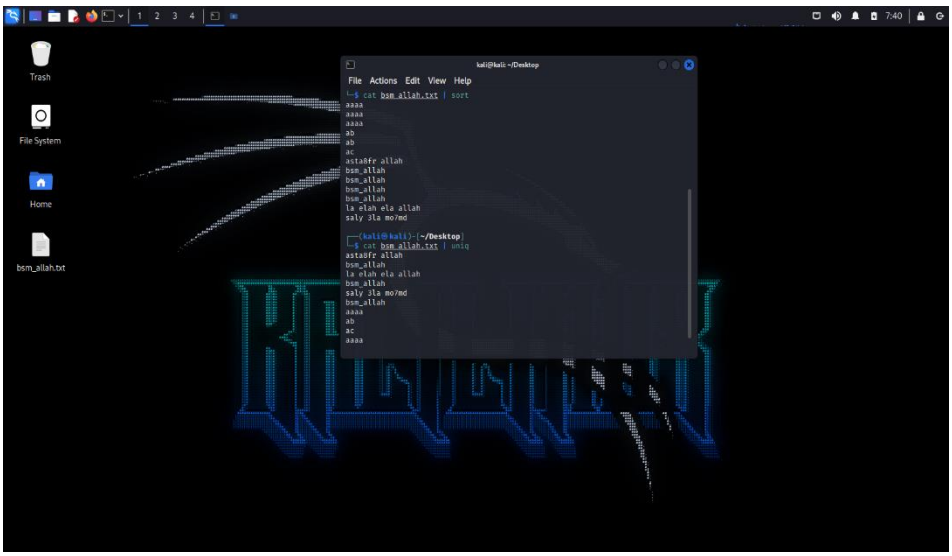
Cut

Awk

Base64 encoding algorithm

لَا يُؤْمِنُ أَحَدُكُمْ، حتَّى يُحِبَّ لأخِيهِ ما يُحِبُّ لِنَفْسِهِ.

Sort Command



Sort command is used to sort a file, arranging the records in a particular order.

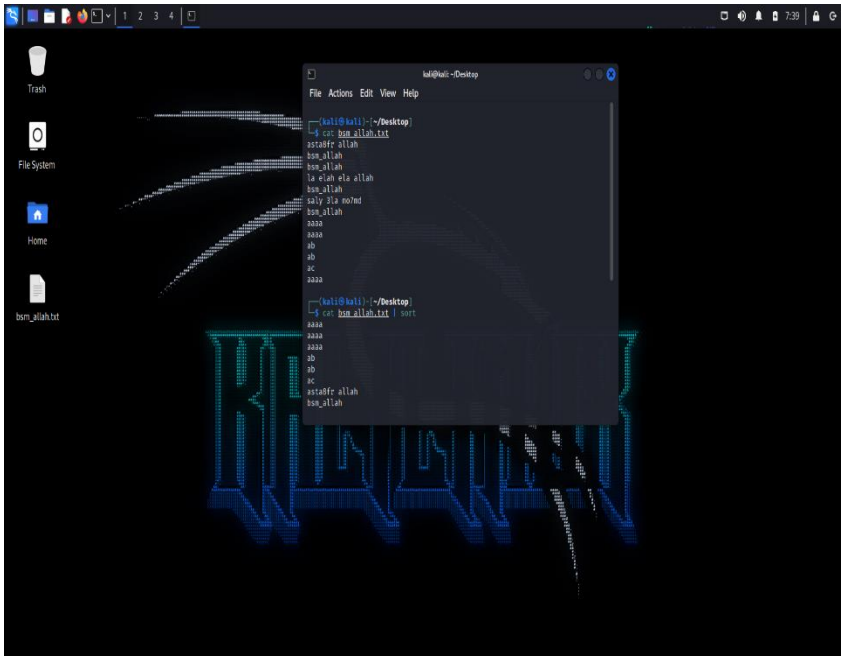
By default, the sort command sorts files assuming the contents are ASCII.

Using options in sort command, it can also be used to sort numerically.

هيرتب الكلام اللي في الملف ابجديا ده طبعا غير الاختيارات اللي جوه بنتكلم عن الاستخدام ده فقط

"cat text.txt | sort"

Uniq Command



The uniq command in Linux is a command line utility that reports or filters out the repeated lines in a file.

In simple words, uniq is the tool that helps to detect the adjacent duplicate lines and deletes the duplicate lines.

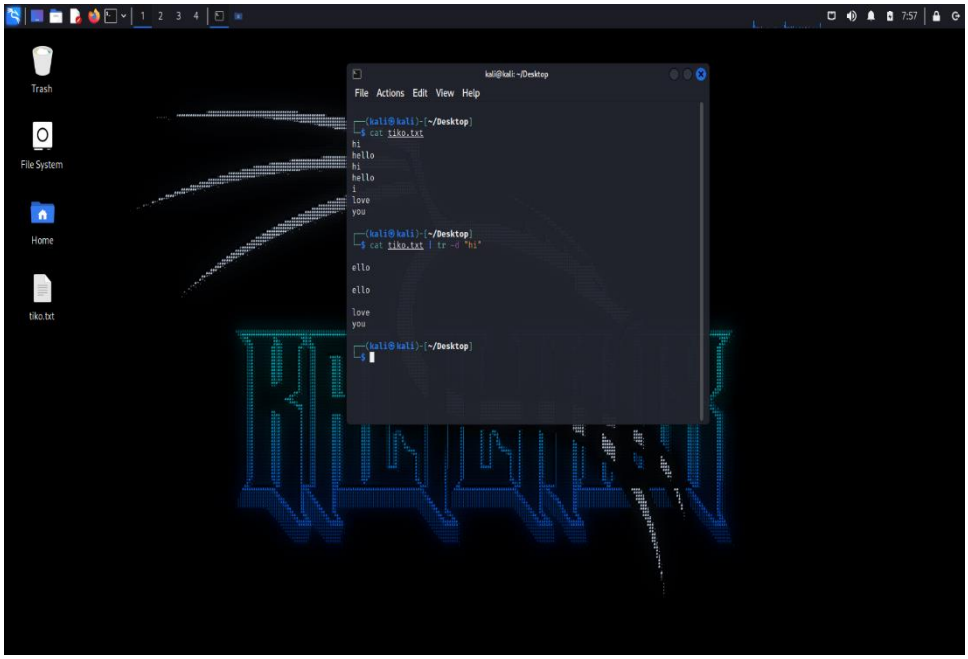
uniq filters out the adjacent matching lines from the input file(that is required as an argument) and writes the filtered data to the output file.

هتطلعلك الحاجات اللي في الملف بدون تكرار ولكن لاحظ ده لو خط متكرر تحت بعضه على طول لكن لو فرق واحد بس مش هتمسحه

"cat text.txt | uniq"

لَا يُؤْمِنُ أَحَدُكُمْ، حتَّى يُحِبَّ لأخِيهِ ما يُحِبُّ لِنَفْسِهِ.

tr Command



The tr command in UNIX is a command line utility for translating or deleting characters.

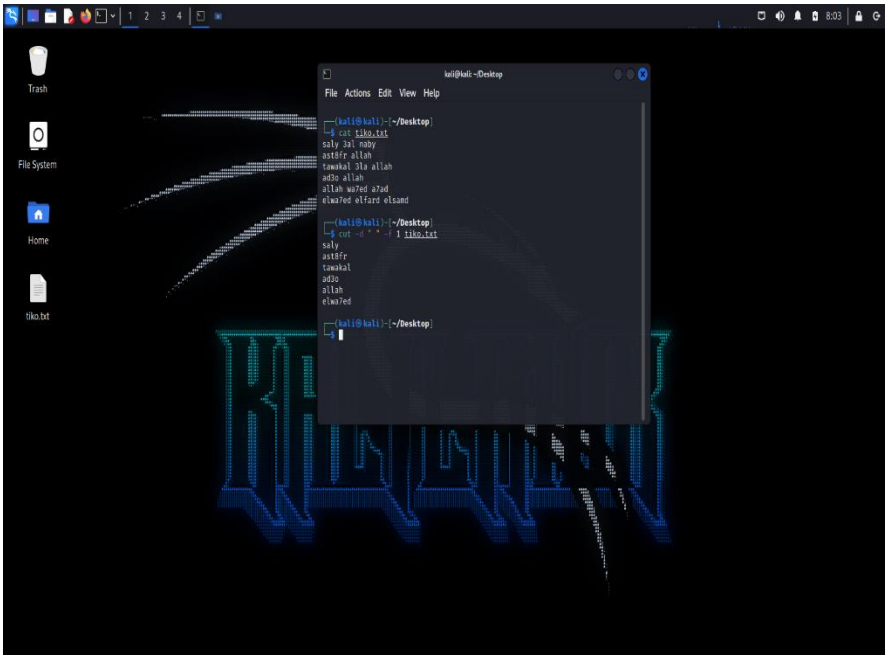
It supports a range of transformations including uppercase to lowercase, squeezing repeating characters, deleting specific characters and basic find and replace.

It can be used with UNIX pipes to support more complex translation. tr stands for translate.

ملهاش حاجه اساسيه زي اللي فاتوا لا دي لازم تختار اختيار ليها فنختار اختيار انها تمسح

cat الملف | tr -d "اللي هنمسحه"

Cut Utility



The cut command in UNIX is a command for cutting out the sections from each line of files and writing the result to standard output.

It can be used to cut parts of a line by byte position, character and field. Basically, the cut command slices a line and extracts the text. It is necessary to specify

وَمَا خَلَقْتُ الْجِنَّ وَالْإِنسَ إِلَّا لِيَعْبُدُونِ

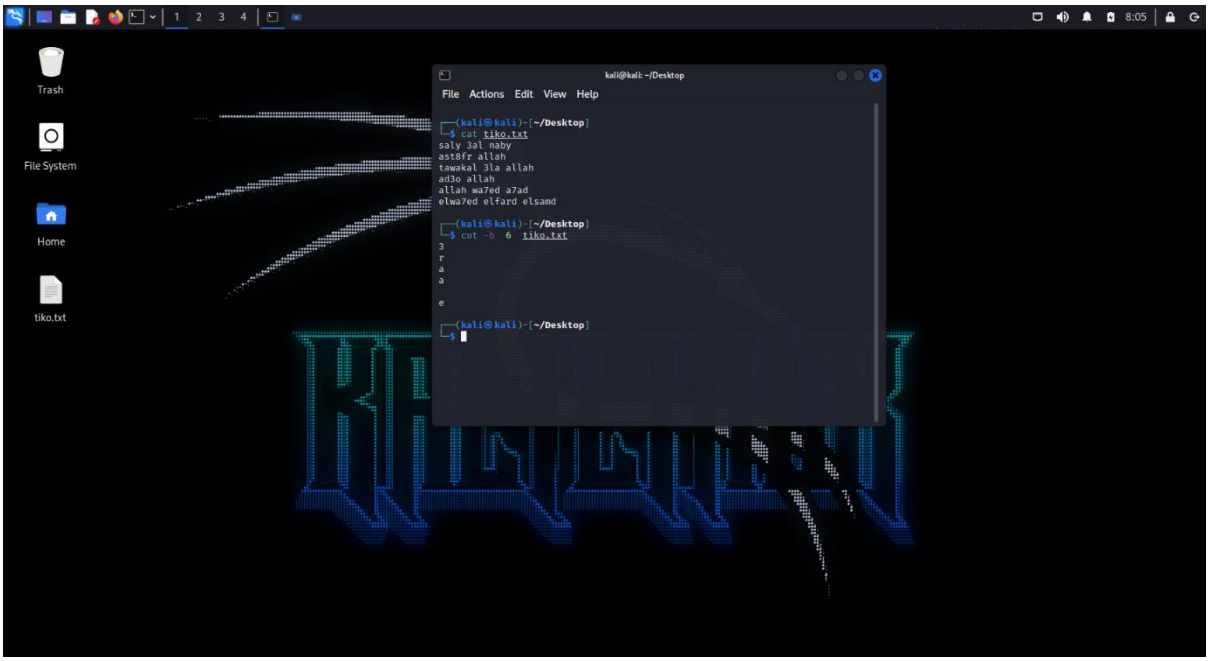
لَا يُؤْمِنُ أَحَدُكُمْ، حتَّى يُحِبَّ لأخِيهِ ما يُحِبُّ لِنَفْسِهِ.

options with commands otherwise it gives errors.

If more than one file name is provided then data from each file is not preceded by its file name.

لا تَحاسَدُوا، ولا تَناجَشُوا، ولا تَباغَضُوا، ولا تَدابَرُوا، ولا يَبِعْ بَعْضُكُمْ علَى بَيْعِ بَعْضٍ، وكُونُوا عِبادَ اللهِ إخْوانًا. المُسْلِمُ أخُو المُسْلِمِ، لا يَظْلِمُهُ، ولا يَخْذُلُهُ، ولا يَحْقِرُهُ. التَّقْوَى هاهُنا. ويُشِيرُ إلى صَدْرِهِ ثَلاثَ مَرَّاتٍ. بحَسْبِ امْرِئٍ مِنَ الشَّرِّ أنْ يَحْقِرَ أخاهُ المُسْلِمَ. كُلُّ المُسْلِمِ علَى المُسْلِمِ حَرامٌ؛ دَمُهُ، ومالُهُ، وعِرْضُهُ.

أنَّ رجلًا قال : يا رسولَ اللهِ قُلْ لي قولًا وأقْلِلْ لعلِّي أعِيه قال لا تغضبْ . فأعاد عليه مرارًا ، كلُّ ذلك يقولُ : لا تغضَبْ .



زي اللي قبليه مينفعش تكتبه كده و تسيبه لازم تختار اختيار و هنشوف اختيارين اختيار انه يطلع حروف معينه و اختيار انه يطلع كلمات معينه

و طبعا كل متحب تتعلم اكتر عن الامر

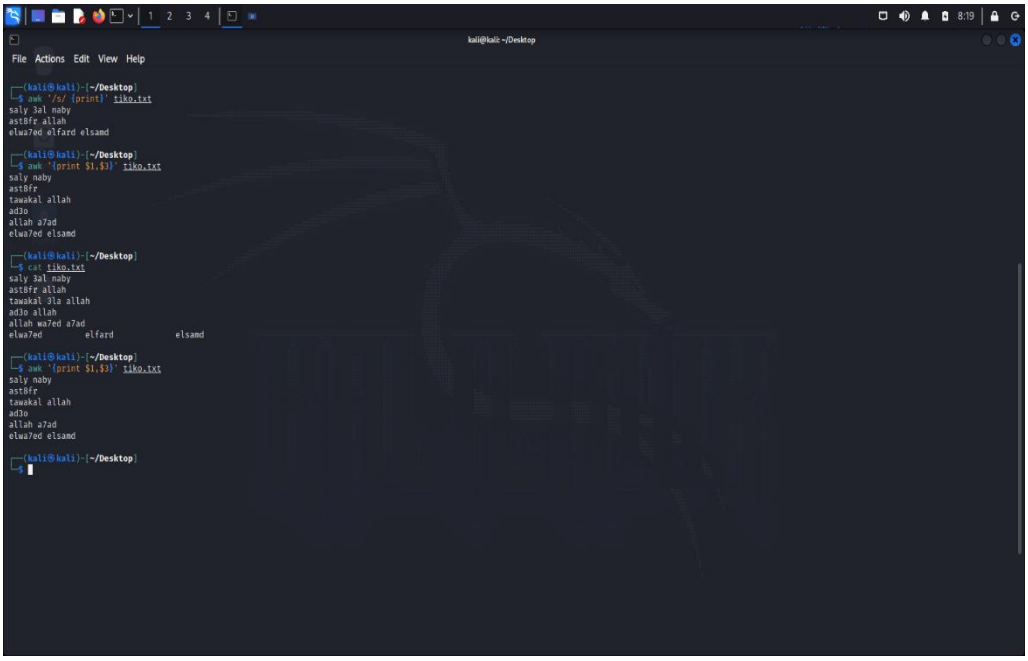
cut --help :)

وَالَّذِينَ إِذَا فَعَلُوا فَاحِشَةً أَوْ ظَلَمُوا أَنفُسَهُمْ ذَكَرُوا اللَّهَ فَاسْتَغْفَرُوا لِذُنُوبِهِمْ وَمَن يَغْفِرُ الذُّنُوبَ إِلَّا اللَّهُ وَلَمْ يُصِرُّوا عَلَىٰ مَا فَعَلُوا وَهُمْ يَعْلَمُونَ

وَمَا خَلَقْتُ الْجِنَّ وَالْإِنسَ إِلَّا لِيَعْبُدُونِ

لَا يُؤْمِنُ أَحَدُكُمْ، حتَّى يُحِبَّ لأخِيهِ ما يُحِبُّ لِنَفْسِهِ.

Awk Utility

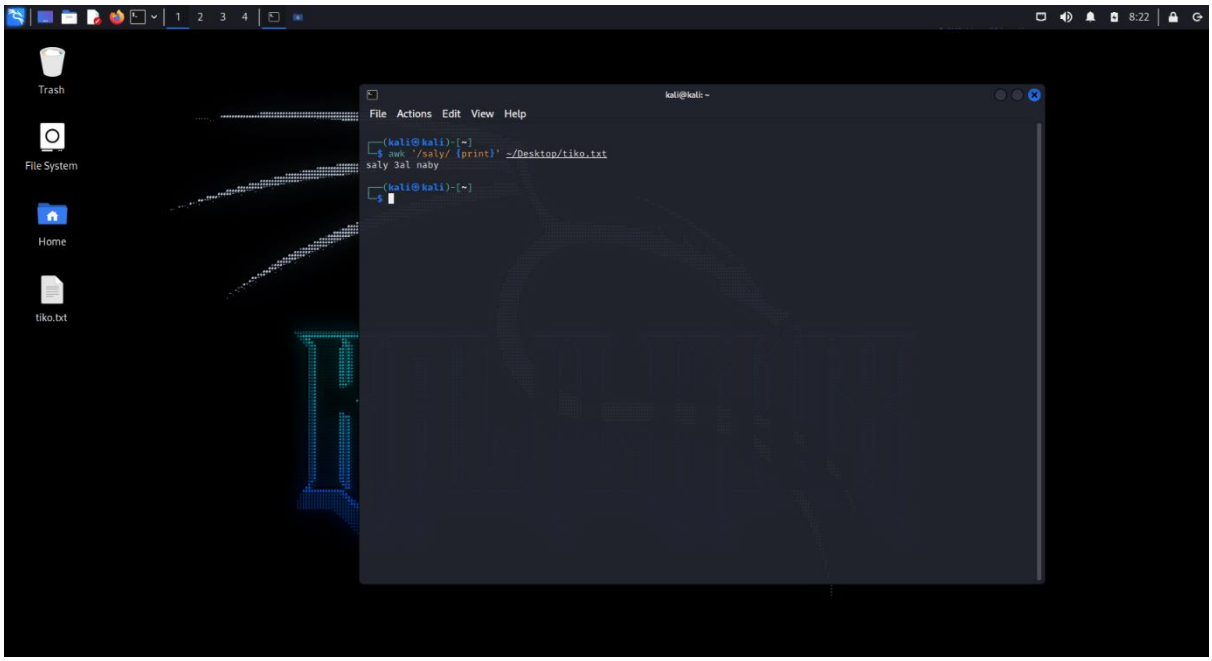


Awk is a utility that enables a programmer to write tiny but effective programs in the form of statements that define text patterns that are to be searched for in each line of a document and the action that is to be taken when a match is found within a line.

Awk is mostly used for pattern scanning and processing.

It searches one or more files to see if they contain lines that match with the specified patterns and then perform the associated actions.

Awk command will be as follows:



awk options 'selection _criteria {action }' input-file >>>>> general form

وَمَا خَلَقْتُ الْجِنَّ وَالْإِنسَ إِلَّا لِيَعْبُدُونِ

لَا يُؤْمِنُ أَحَدُكُمْ، حتَّى يُحِبَّ لأخِيهِ ما يُحِبُّ لِنَفْسِهِ.

طيب تعالى نشوف استخدامين من استخداماتها الاول هو اننا عايزين نظهر السطور اللي فيها حرف معين او كلمه معينه

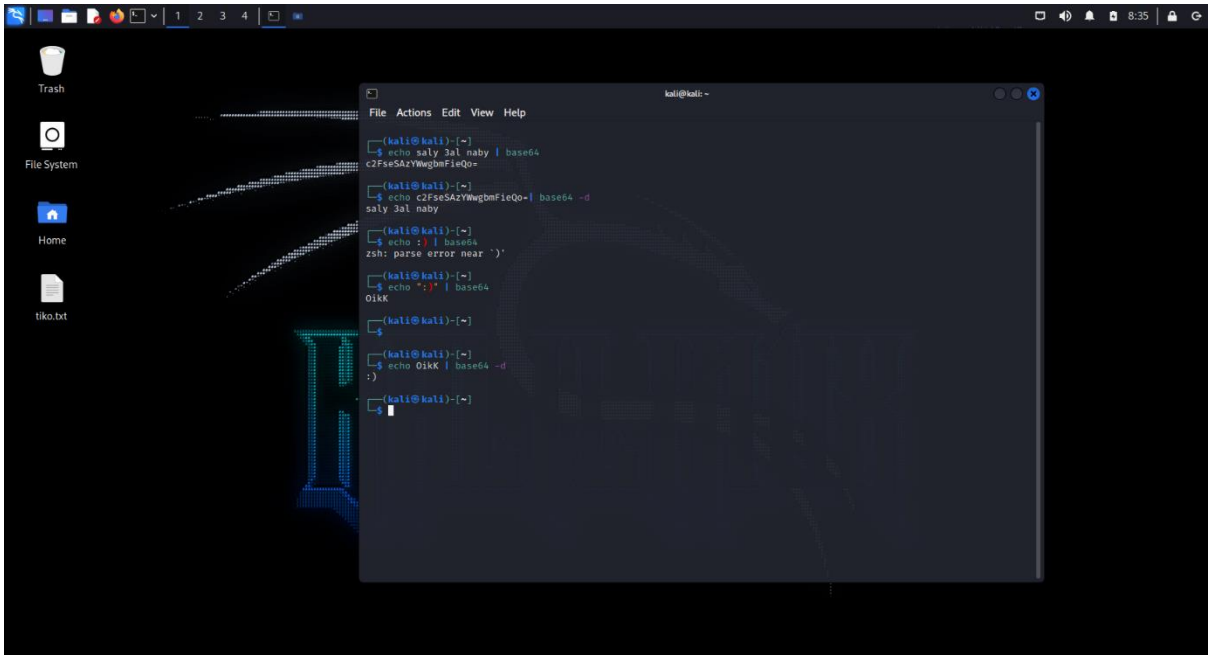
In Awk there are some built-in variables we can use like NR which will print the line number to print the line number and line content we can use the following command.

هتستخدمه علشان تطلع السطور مترقمه و لاحظ علامه الدولار بعديها لو كتبت صفر فانت كده بتقله يطبع السطر كله حطيت بقى واحد او اتنين او غيره هيطبع الكلمه بالرقم ده مع اهمال طبعا المسافات

لاحظ لما تدور بكلمه هو حساس لو كان الحرف كبير ولا صغير

upper or lower case يا محنك منك ليه :)

Base64 Encoding Algorithm



Base64 is an encoding algorithm that allows you to transform any characters into an alphabet that consists of Latin letters, digits, plus, and slash.

وَمَا خَلَقْتُ الْجِنَّ وَالْإِنسَ إِلَّا لِيَعْبُدُونِ

لَا يُؤْمِنُ أَحَدُكُمْ، حتَّى يُحِبَّ لأخِيهِ ما يُحِبُّ لِنَفْسِهِ.

Thanks to it, you can convert Chinese characters, emoji, and even images into a “readable” string, which can be saved or transferred anywhere.

You can decode any text from base64 using the base64 command with -d as argument.

echo "sentence or words needed to encode or decode" | base64 "type -d if you want to decode leave it without adding anything else to encode"

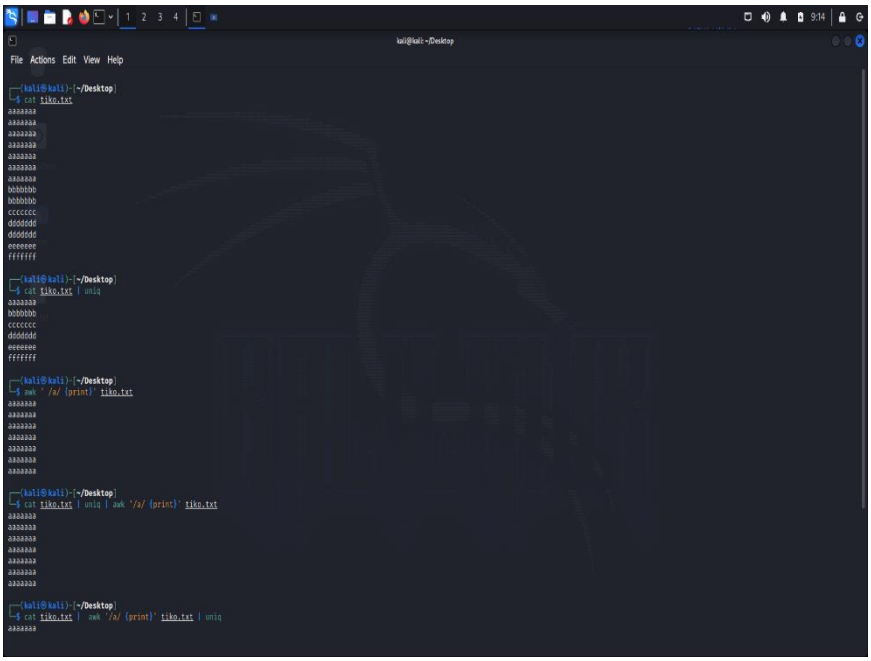
وَقَالَ الشَّيْطَانُ لَمَّا قُضِيَ الْأَمْرُ إِنَّ اللَّهَ وَعَدَكُمْ وَعْدَ الْحَقِّ وَوَعَدتُّكُمْ فَأَخْلَفْتُكُمْ ۖ وَمَا كَانَ لِيَ عَلَيْكُم مِّن سُلْطَانٍ إِلَّا أَن دَعَوْتُكُمْ فَاسْتَجَبْتُمْ لِي ۖ فَلَا تَلُومُونِي وَلُومُوا أَنفُسَكُم ۖ مَّا أَنَا بِمُصْرِخِكُمْ وَمَا أَنتُم بِمُصْرِخِيَّ ۖ إِنِّي كَفَرْتُ بِمَا أَشْرَكْتُمُونِ مِن قَبْلُ ۗ إِنَّ الظَّالِمِينَ لَهُمْ عَذَابٌ أَلِيمٌ

إِنَّ اللَّهَ وَمَلَائِكَتَهُ يُصَلُّونَ عَلَى النَّبِيِّ ۚ يَا أَيُّهَا الَّذِينَ آمَنُوا صَلُّوا عَلَيْهِ وَسَلِّمُوا تَسْلِيمًا

try decoding this :
c2FseSAzYWwgbmFieQo=

ctrl + shift + c >>> to copy

ctrl + shift + v >>> to paste :)



مفاجأه كنت سايبهالك لحد متكون اتعلمتلك حبه :)

تقدر تدمج كذا امر سوا بص على الصوره التاليه :)

لاحظ من الصوره ترتيب الاوامر بيفرق :)

What is meant by the User?

A user is anyone who uses a computer. In this case, we are describing the names which represent those users. It may be Ahmed or joe or any other name, and they may use the names Dragonlady or Pirate in place of their real name. All that matters is that the computer has a name for each account it creates, and it is this name by which a person gains access to use the computer. Some system services also run using restricted or privileged user accounts (admin or root account).

How are users managed in Linux?

وَمَا خَلَقْتُ الْجِنَّ وَالْإِنسَ إِلَّا لِيَعْبُدُونِ

لَا يُؤْمِنُ أَحَدُكُمْ، حتَّى يُحِبَّ لأخِيهِ ما يُحِبُّ لِنَفْسِهِ.

Managing users is done for the purpose of security by limiting access in certain specific ways, having full control over the users and applying a good security policy and rules is something important. The superuser (root) has complete access to the operating system and its configuration; it is intended for administrative use only. Unprivileged users can use the su and sudo programs for controlled privilege elevation.

What is meant by Group?

In Linux, a group is a collection of users or we can say it is like a club containing specific members (users). The main purpose of the groups is to define a set of privileges like read, write, or execute permission for a given resource that can be shared among the

users within the group. Users can be added to an existing group to utilize the privileges it grants, for every group there is a group ID, a group ID is an identifier for the group and not necessarily unique, it could be found in the /etc/groups file.

مختصر الرغي ده :)

في حاجه اسمها مستخدم ده اسم و باسورد بتدخلهم على اللينكس كلمستخدم ليه صلاحيات معينه يقدر يعملها بمعنى

عندي موظفين في شركه عايز اخلي قسم المحاسبه يقدر يقرأ التقارير اللي جايه من قسم تاني فقط و لكن ميعدلش فيها و لا يكتب في الملف بتاعهم خلاص هديهم اكونتات بتدي صلاحيه في ملف القسم التاني

read only

و هكذا في باقي الصلاحيات و ده ممكن اعمله في كذا اكونت و اجمع الاكونتات دي كلها في مجموعه

"group"

و بكده هقدر ان شاء الله اخليهم كلهم في المجموعه دي بنفس الصلاحيات

و عندي الاكونت اللي مفتوحله كل الصلاحيات و اللي يقدر يعمل اي حاجه في النظام و هو

root

بس كده :)

Types Of Groups :

There are two types of groups in Linux :

The Primary Group:

it is also called a private group, each user must have a primary group and it is automatically generated by the operating system when user is created, to make the importance of the primary groups clear imagine that a user created a set of files, the operating system will associate the primary group of the user with all the files to track them.

لَا يُؤْمِنُ أَحَدُكُمْ، حتَّى يُحِبَّ لأخِيهِ ما يُحِبُّ لِنَفْسِهِ.

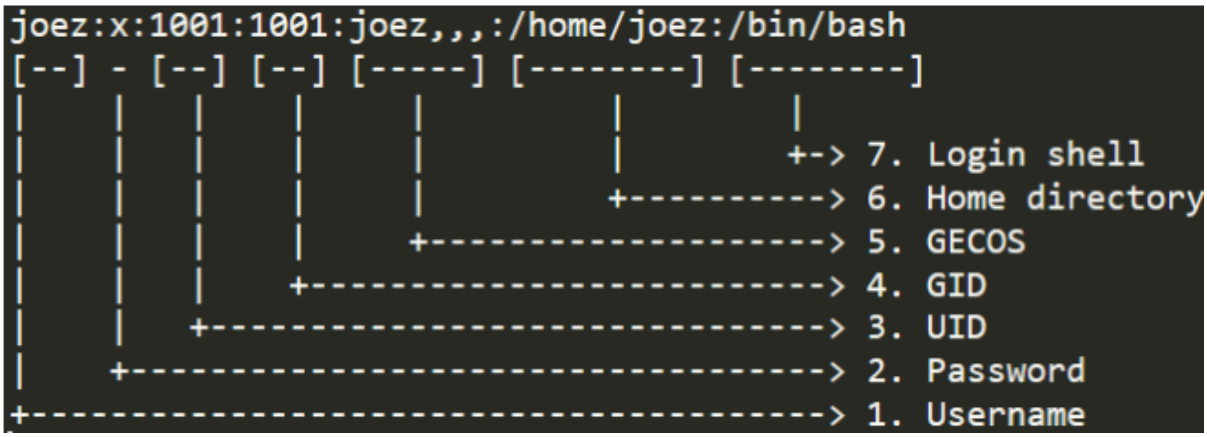
The Secondary Group:

secondary groups are optional groups, the users can be added to a single secondary group or many secondary groups, secondary groups grants a set of privileges for all the group members, for example, if a group has the permissions to read a specific file all the members can read that file, secondary groups enhances the security level of the operating system.

two important files here in Linux.

`/etc/shadow`: is a text file that contains information about the system's users' passwords. It is owned by user root and group shadow, every line in this file contains an entry every entry is responsible for representing a user account.

`/etc/passwd`: is a plain text-based database that contains information for all user accounts on the system, also an entry in each line. It is owned by root. The file can only be modified by root or users with sudo privileges and all users can read it.



/etc/passwd format :

Username: The string you type when you log into the system. Each username must be a unique string on the machine. The maximum length of the username is restricted to 32 characters.

Password: In older Linux systems, the user's encrypted password was stored in the /etc/passwd file. On most modern systems, this field is set to x, and the user password is stored in the /etc/shadow file.

UID: The user identifier is a unique decimal number assigned to each user. It is used by the operating system to refer to a user.

GID: The user's group identifier number, referring to the user's primary group. When a user creates a file, the file's group is set to this group.

GECOS: This field contains a list of comma-separated values which will contain values like phone number, full name, the value of this field is a string value and it cannot contain colons.

لَا يُؤْمِنُ أَحَدُكُمْ، حتَّى يُحِبَّ لأخِيهِ ما يُحِبُّ لِنَفْسِهِ.

Home directory: The absolute path to the user's home directory. It contains the user's files and configurations. By default, the user home directories are named after the name of the user and created under the /home directory and the value is a character string.

Login shell: The absolute path to the user's login shell. This is the shell that is started when the user logs into the system. On most Linux distributions, the default login shell is Bash.

permissions in linux :

Since Linux is a multi-user operating system (which means multiple users can have access to the system at, same time), for efficient security, it implements file ownership and file permission as a feature to provide a secure way of storing and accessing files.

File Ownership in Linux

Linux assigns three types of ownership to every file and directory:

Owners

The user who creates a file or directory is considered the owner and, the owner's permission assigned to the file or directory defines what action the owner can perform on the file or directory

Groups

A group contain multiple users with the same permission assigned to every member of the group. The permissions define what action any member of the group can perform on a file or directory.

Others (world)

Others include everyone else who is not a member of any group or an owner of a file/directory. For security purposes, always be mindful of the permission you assign here, as the file/directory permission defines what action anybody (the world) can perform on a file or directory.

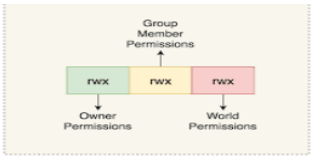
يا أيُّها النَّاسُ إنَّ اللهَ طيّبٌ لا يقبلُ إلَّا طيّبًا ، وإنَّ اللهَ أمرَ المؤمنينَ بما أمرَ بِه المرسلينَ فقالَ يَا أَيُّهَا الرُّسُلُ كُلُوا مِنَ الطَّيِّبَاتِ وَاعْمَلُوا صَالِحًا إِنِّي بِمَا تَعْمَلُونَ عَلِيمٌ وقالَ يَا أَيُّهَا الَّذِينَ آمَنُوا كُلُوا مِنْ طَيِّبَاتِ مَا رَزَقْنَاكُمْ قالَ وذَكرَ الرَّجلَ يُطيلُ السَّفرَ أشعثَ أغبرَ يمدُّ يدَه إلى السَّماءِ يا ربِّ يا ربِّ ومطعمُه حرامٌ ومشربُه حرامٌ وملبسُه حرامٌ وغذِّيَ بالحرامِ فأنَّى يستجابُ لذلِك

وَمَا خَلَقْتُ الْجِنَّ وَالْإِنسَ إِلَّا لِيَعْبُدُونِ

لَا يُؤْمِنُ أَحَدُكُمْ، حتَّى يُحِبَّ لأَخِيهِ ما يُحِبُّ لِنَفْسِهِ.

File Permissions in Linux

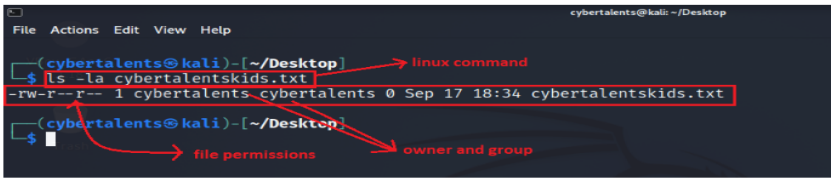
Linux assigns three types of permissions to every file and directory:



Read

Read gives users the privilege to view a file or list the contents of a directory.

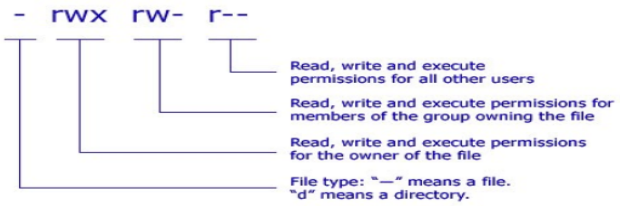
To view the list of permissions, in Linux use the command **ls -la filename**.



Write

Write gives users the privilege to edit a file or modify a directory.

These are the permissions points in the result of the command.

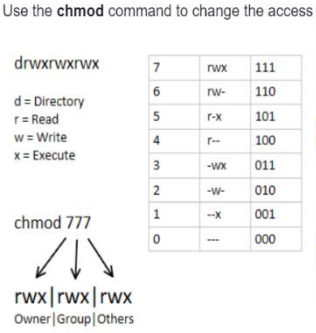


Execute

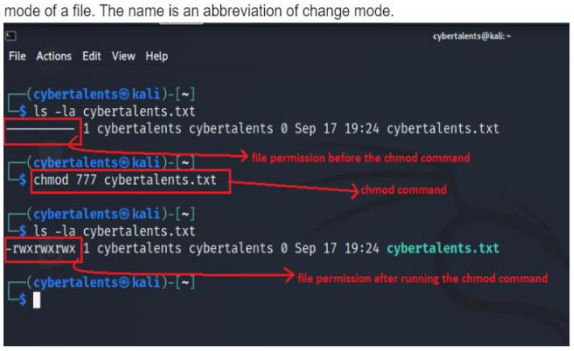
Execute gives users the privilege to run a file as a computer program.

How to Change File Permission in Linux

Use the **chmod** command to change the access mode of a file. The name is an abbreviation of change mode.



7	rwx	111
6	rw-	110
5	r-x	101
4	r--	100
3	-wx	011
2	-w-	010
1	--x	001
0	---	000



مختصر الرغي :)

بكل بساطه لينكس هو نظام بيكون فيه كذا مستخدم و كل مستخدم بصلاحيات مختلفه في الملفات سواء يقرأ او يكتب او يشغل برنامج معين

مثال بسيط خش .... root بأي مستخدم غير ال

و جرب تفتح ملف /etc/shadow :)

علشان كده كل ملف بيكون النظام مديله صلاحيات لصاحبه يقدر يعمل فيه ايه و صلاحيات للمجموعات على النظام و صلاحيات لأي حد تاني على النظام يقدر يعمل ايه في الملف

و ممكن كل مستخدم ياخد اكتر من صلاحيه و بس كده :)

الطُّهورُ شطْرُ الإيمانِ ، والحمدُ للهِ تملأُ الميزانَ ، وسُبحانَ اللهِ والحمدُ للهِ تَملآنِ ما بين السماءِ والأرضِ ، والصلاةُ نورٌ ، والصدَقةُ بُرهانٌ ، والصبْرُ ضِياءٌ ، والقُرآنُ حُجَّةٌ لكَ أوْ عليكَ ، كلُّ الناسِ يَغدُو ، فبائِعٌ نفسَهُ ، فمُعتِقُها أوْ مُوبِقُها

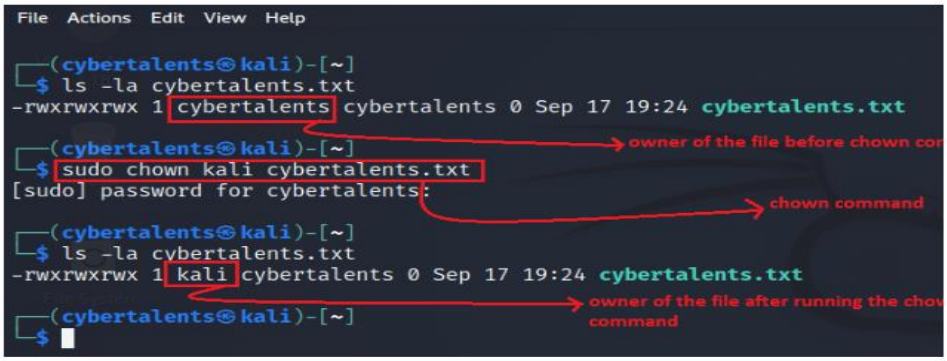
وَمَا خَلَقْتُ الْجِنَّ وَالْإِنسَ إِلَّا لِيَعْبُدُونِ

لَا يُؤْمِنُ أَحَدُكُمْ، حتَّى يُحِبَّ لأخِيهِ ما يُحِبُّ لِنَفْسِهِ.

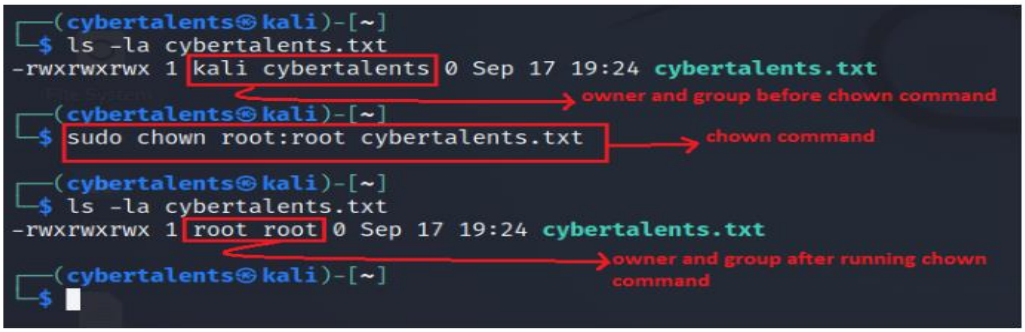
كنتُ خلفَ رسولِ اللهِ صلَّى اللهُ عليه وسلَّمَ يومًا قال يا غلامُ ، إني أعلِّمُك كلماتٍ : احفَظِ اللهَ يحفَظْك ، احفَظِ اللهَ تجِدْه تُجاهَك ، إذا سألتَ فاسألِ اللهَ ، وإذا استعنْتَ فاستعِنْ باللهِ ، واعلمْ أنَّ الأمةَ لو اجتمعتْ على أن ينفعوك بشيءٍ ، لم ينفعوك إلا بشيءٍ قد كتبه اللهُ لك ، وإنِ اجتمعوا على أن يضُرُّوك بشيءٍ لم يضُروك إلا بشيءٍ قد كتبه اللهُ عليك ، (رُفِعَتِ الأقلامُ وجَفَّتِ الصُّحُفَ)

How to Change File and Group ownership in Linux

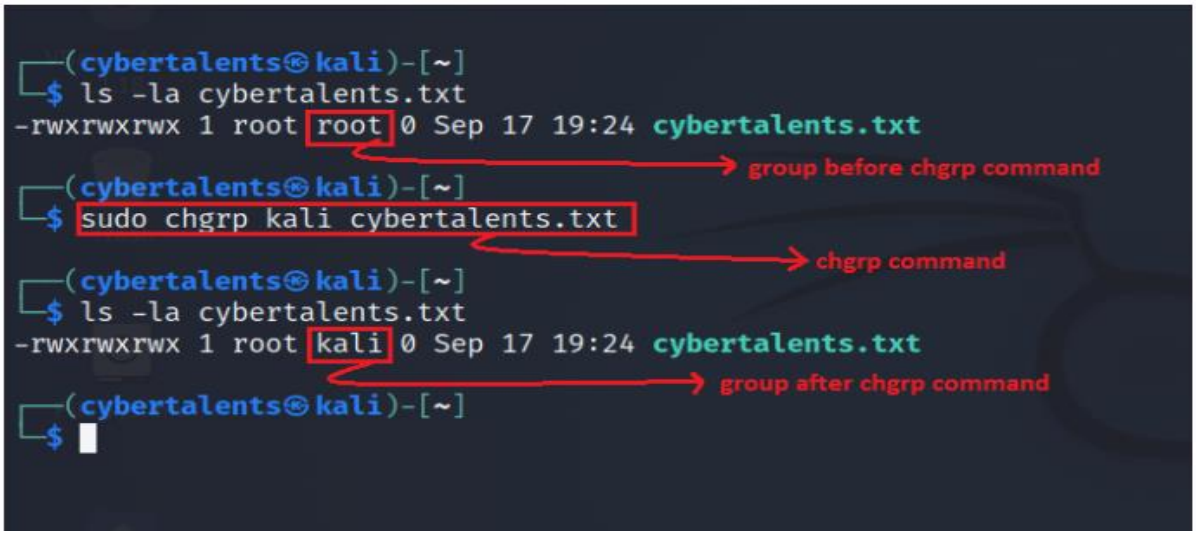
- To change the **ownership** of a file or directory use **chown user filename**.



- To change the **ownership** and **group** of a file or directory use **chown user:group filename**.



- To change only the ownership of a **group**, use the **chgrp group filename**.



لَا يُؤْمِنُ أَحَدُكُمْ، حتَّى يُحِبَّ لأخِيهِ ما يُحِبُّ لِنَفْسِهِ.

وَقَالَ الشَّيْطَانُ لَمَّا قُضِيَ الْأَمْرُ إِنَّ اللَّهَ وَعَدَكُمْ وَعْدَ الْحَقِّ وَوَعَدتُّكُمْ فَأَخْلَفْتُكُمْ ۖ وَمَا كَانَ لِيَ عَلَيْكُم مِّن سُلْطَانٍ إِلَّا أَن دَعَوْتُكُمْ فَاسْتَجَبْتُمْ لِي ۖ فَلَا تَلُومُونِي وَلُومُوا أَنفُسَكُم ۖ مَّا أَنَا بِمُصْرِخِكُمْ وَمَا أَنتُم بِمُصْرِخِيَّ ۖ إِنِّي كَفَرْتُ بِمَا أَشْرَكْتُمُونِ مِن قَبْلُ ۗ إِنَّ الظَّالِمِينَ لَهُمْ عَذَابٌ أَلِيمٌ

What is a process?

A process is an instance of a program currently running in the form of a thread(s). A process is an active entity while a program is a passive entity. Depending on the environment, a process can be uni-threaded (consisting of a single thread) or multithreaded (consisting of multiple threads).

In Linux, there are various commands that are used for process manipulation. There are commands that enable a user to view the list of processes and their information, delay the start of a particular process, and terminate or stop a process from further execution.

In simple terms, any command that you give to your Linux machine starts a new process

ملخص الرغي :)

بكل بساطه عندك عمليات بتحصل في الجهاز يعني ايه عمليه بكل بساطه لو انت فاتح الملف بتاعك و بتدور جواه على ملف معين مش فاكر حطيته فين فبتكتب اسمه

و تدور عليه اهو الجهاز و هو بيدور ده اسمه عمليه و العمليه بيبقى اسمها تفاعليه لانها بتحصل لما يبقى في تفاعل ادى لحدوثها لكن البرنامج هو غير تفاعلي و لما تشغله بيحصل عمليه العمليه دي بقى تفاعليه شوفت ازاي :)

فالخلاصه اي حاجه بتعملها في النظام بيبقى عمليه جديده :)

و اه انواع العمليات بيقلك خيط واحد او كذا خيط (ترجمه حرفيه ولا اجدعها جوجل :))بص يسيدي من الاخر في عمليه بتحصل بين طرف و طرف تاني فقط او عمليه بين طرف و عده اطراف بس كده :)

Linux Process Manipulation :

Below are two ways to start a process (run a command):

Foreground Processes

A foreground process is any command or task you run directly and wait for it to complete. Some foreground processes show some type of user interface that supports ongoing user interaction, whereas others execute a task and "freeze" the computer while it completes that task. Thus, there has to be a user connected to the system to start such processes since they are not started automatically as part of the system functions/services. They are also referred to as interactive processes.

Running a Foreground Process

لَا يُؤْمِنُ أَحَدُكُمْ، حتَّى يُحِبَّ لأخِيهِ ما يُحِبُّ لِنَفْسِهِ.

To start a foreground process, you can either run it from the dashboard, or you can run it from the terminal.

Background Processes

Unlike with a foreground process, the terminal does not have to wait for a background process to end before it can run more processes. Within the limit of the amount of memory available, you can enter many background commands one after another. To run a command as a background process, type the command and add a space and an ampersand to the end of the command. These are also referred to as non-interactive/automatic processes.

Running a Background process

If you start a foreground program/process from the terminal, then you cannot work on the terminal, till the program is up and running.

In particular, data-intensive tasks take lots of processing power and may even take hours to complete. Since you do not want your terminal to be held up for such a long time, it is recommended that you run the program and send it to the background so that the terminal remains available to you. Follow the steps below:

Start the program and press ctrl + z (*)

Type bg and send the process to the background (*)

ملخص الرغي :)

بكل بساطه لينكس بيعالج العمليات بطريقتين اما انك تكون بتعالجها قدامك بمعنى فاتح برنامج شايفه و هو شغال قدامك و ده العادي او لا عايز تشغل برنامج يعمل مهمه تاخد وقت

لحد متخلص فلا انا اقوم مخليها تشتغل في الخلفيه و اشتغل براحتي عادي و ده ازاي هتلاقي مشروح في السطرين اللي جنبهم terminal المهمه دي هتعطلي كده ال

بس كده (*) :)

دعْ ما يُرِيبُكَ إلى ما لا يُرِيبُكَ فإنَّ الصدقَ طُمأنينةٌ وإنَّ الكذبَ رِيبَةٌ

Types of Processes:

1. Parent process:

The process is created by the user on the terminal. All processes have a parent process, If it was created directly by the user then the parent process will be the kernel process.

العمليه الاب لكل العمليات و اللي بيتم عملها من المستخدم و بتسمى عمليه كرنيل :)

2. Child process:

This is a process created by another process (by its parent process). All child processes have a parent process.

وَمَا خَلَقْتُ الْجِنَّ وَالْإِنسَ إِلَّا لِيَعْبُدُونِ

The example is given above, the process having PID 28500(last row) is a child process of the process having PID 26544.

عمليه تابعه للعمليه الاب من الاخر عمليه ادت لحدوث عمليه اخرى بس كده :)

3. Orphan process:

After completing its execution a child process is terminated or killed and SIGCHLD updates the parent process about the termination and thus can continue the task assigned to it. But sometimes, when the parent process is killed before the termination of the child process, the child processes become orphan processes, with the parent of all processes “init” process (PID 0), becomes their new PID.

في العادي عمليه الطفل لما بتنتهي بتبعت للاب انها انتهت بس افرض العمليه الاب اغلقت قبل الابن متنتهي بكل بساطه بتبقى عمليه يتيمه و يتم ربطها بالعمليه الاب لكل العمليات

عمليه init :)

4. Zombie process:

A process that is killed but still shows its entry in the process status or the process table is called a zombie process, they are dead and are not used. They have Zero CPU consumption.

عمليه انتهت و لكن لسه مكتوبه في السجل عندي و الحمد لله مبتستهلكش من الطاقه :)

5. Daemon process:

They are system-related background processes that often run with the permissions of root and services requests from other processes, they usually run in the background and wait for processes they can work along with for ex print daemon. A Daemon process can be recognized if it has “?” in its TTY field (6th column)

عمليه بتشتغل في الخلفيه من عمليات النظام الاساسيهو بتكون في الخلفيه منتظره التفعيل :)

States of a Process in Linux

During execution, a process changes from one state to another depending on its environment/circumstances. In Linux, a process has the following possible states:

Running – here it’s either running (it is the current process in the system) or it’s ready to run (it’s waiting to be assigned to one of the CPUs).

العمليه شغاله او مستعده منظره منك امر تشغيلها :)

Waiting – in this state, a process is waiting for an event to occur or for a system resource. Additionally, the kernel also differentiates between two types of waiting processes; interruptible waiting processes – can be interrupted by signals and uninterruptible waiting processes – are waiting directly on hardware conditions and cannot be interrupted by any event/signal.

العمليه منتظره حدوث حدث ما و عندك نوعين نوع ممكن قابل للمقاطعه بارسال اشاره ليه و نوع تاني غير قابل للمقاطعه مرتبط بالهاردوير مباشره

لَا يُؤْمِنُ أَحَدُكُمْ، حتَّى يُحِبَّ لأخِيهِ ما يُحِبُّ لِنَفْسِهِ.

Stopped – in this state, a process has been stopped, usually by receiving a signal. For instance, a process that is being debugged.

عمليه توقفت :)

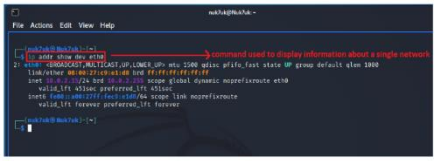
Linux processes are managed using system calls. The following table shows a summary of some common Linux system calls:

System call	Description
pid = fork( )	Create a child process identical to the parent
pid = waitpid(pid, &statloc, opts)	Wait for a child to terminate
s = execve(name, argv, envp)	Replace a process' core image
exit(status)	Terminate process execution and return status
s = sigaction(sig, &act, &oldact)	Define action to take on signals
s = sigreturn(&context)	Return from a signal
s = sigprocmask(how, &set, &old)	Examine or change the signal mask
s = sigpending(set)	Get the set of blocked signals
s = sigsuspend(sigmask)	Replace the signal mask and suspend the process
s = kill(pid, sig)	Send a signal to a process
residual = alarm(seconds)	Set the alarm clock
s = pause( )	Suspend the caller until the next signal

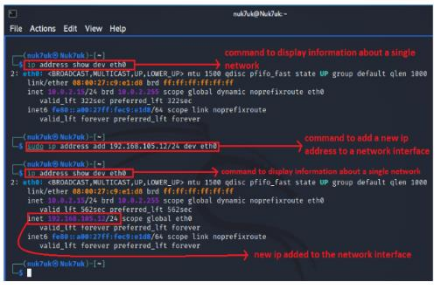
Display and Modify Information Associated to a Network Interface:

"ip" command :

"ip" command is a replacement for the traditional "ifconfig" command, ip which stands for Internet Protocol, is a tool used to configure and analyze a network interface, to bring interfaces up or down, assign and remove addresses and routes, manage ARP cache, and much more.



- To add an IP address to a network interface on your machine, use **ip address add <new_ip> dev <interface>** e.g **sudo ip address add 196.168.105.12/24 dev eth0.**



To view all the interfaces and the assigned ip address, subnet and default gateway we can use the command

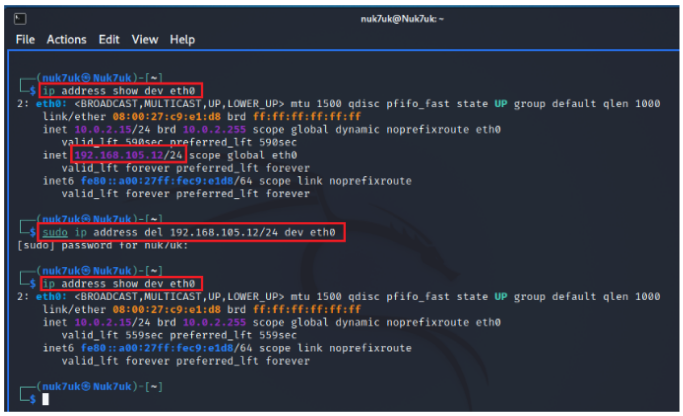
ip address, ip addr or ip a

To display information about a single network interface, use ip addr show dev <interface_name> e.g ip addr show dev eth0.

وَمَا خَلَقْتُ الْجِنَّ وَالْإِنسَ إِلَّا لِيَعْبُدُونِ

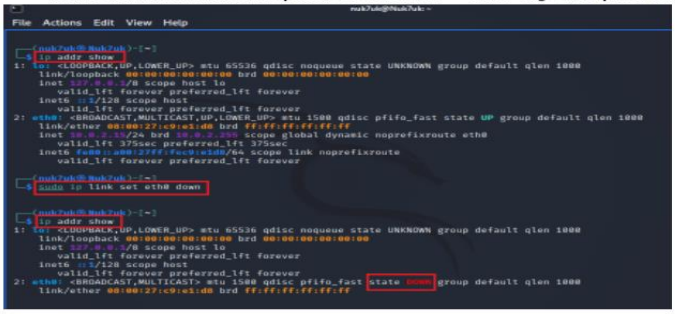
لَا يُؤْمِنُ أَحَدُكُمْ، حتَّى يُحِبَّ لأخِيهِ ما يُحِبُّ لِنَفْسِهِ.

- To delete an IP address from a network interface on your machine, use **ip address del <new_ip> dev <interface>** e.g **sudo ip address del 196.168.105.12/24 dev eth0.**

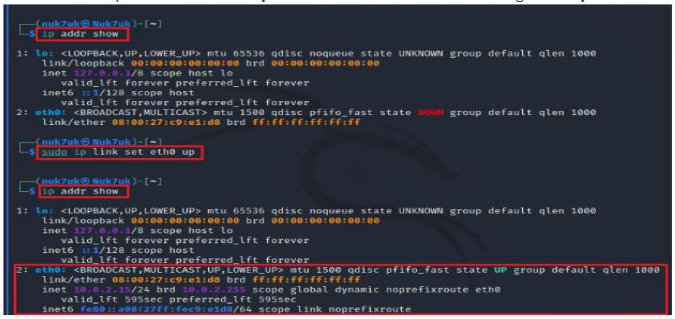


- To take down an interface use **ip link set <interface> <state>** e.g **sudo ip link set eth0 down.**

- To take down an interface use **ip link set <interface> <state>** e.g **sudo ip link set eth0 down.**



- To take up an interface use **ip link set <interface> <state>** e.g **sudo ip link set eth0 up.**



لَا يُؤْمِنُ أَحَدُكُمْ، حتَّى يُحِبَّ لأخِيهِ ما يُحِبُّ لِنَفْسِهِ.

أَفَحَسِبْتُمْ أَنَّمَا خَلَقْنَاكُمْ عَبَثًا وَأَنَّكُمْ إِلَيْنَا لَا تُرْجَعُونَ

"ifconfig" command:

“ifconfig” command like the “ip” command is used to configure, display and control network interfaces. The “ip” command is an alternative to the “ifconfig” command, but with many more functionalities than the “ifconfig” command.

With the “ifconfig”, you can perform some network functionalities, such as displaying or modifying a network interface, displaying mac addresses associated with a network interface, modifying hardware information and much more.

To display information about an interface, use the “ifconfig” command

أَنَّهُ سَمِعَ رَسولَ اللهِ صَلَّى اللَّهُ عليه وسلَّمَ يقولُ: ما نَهَيْتُكُمْ عنْه فَاجْتَنِبُوهُ، وَما أَمَرْتُكُمْ به فَافْعَلُوا منه ما اسْتَطَعْتُمْ، فإنَّما أَهْلَكَ الَّذِينَ مِن قَبْلِكُمْ، كَثْرَةُ مَسَائِلِهِمْ، وَاخْتِلَافُهُمْ علَى أَنْبِيَائِهِمْ. [وفي رواية]: ذَرُونِي ما تَرَكْتُكُمْ. وفي حَدِيثِ هَمَّامٍ: ما تَرَكْتُمْ، فإنَّما هَلَكَ مَن كانَ قَبْلَكُمْ ثُمَّ ذَكَرُوا نَحْوَ: حَدِيثِ الزُّهْرِيِّ، عن سَعِيدٍ وَأَبِي سَلَمَةَ، عن أَبِي هُرَيْرَةَ.

وَمَا خَلَقْتُ الْجِنَّ وَالْإِنسَ إِلَّا لِيَعْبُدُونِ

لَا يُؤْمِنُ أَحَدُكُمْ، حتَّى يُحِبَّ لأخِيهِ ما يُحِبُّ لِنَفْسِهِ.

interact with External Servers from the Terminal:

Ping Command:

Ping command: This is a simple utility used to check whether a network is available and if a host is reachable. With this command, you can test if a server is up and running. It also helps with troubleshooting various connectivity issues.

To use the ping command we can follow the following format

Ping [option] `hostname`

Curl:

This is a command-line tool to transfer data to or from a server, using any of the supported protocols (HTTP, FTP, IMAP, POP3, SCP, SFTP, SMTP, TFTP, TELNET, LDAP or FILE). curl is powered by libcurl. This tool is preferred for automation since it is designed to work without user interaction. curl can transfer multiple files at once.

Curl command can be used in the following way

curl [options] [URL]

Wget:

This is the non-interactive network downloader that is used to download files from the server even when the user has not logged on to the system and it can work in the background without hindering the current process.

Wget command can be used in the following way

wget [options] [URL]

إنَّ أحبَّ الكلامِ إلى اللَّهِ أن يقولَ العبدُ : سبحانَكَ اللَّهمَّ وبحمدِكَ ، وتبارَكَ اسمُكَ ، وتعالى جدُّكَ ، ولا إلَهَ غيرُكَ ، وإنَّ أبغضَ الكلامِ إلى اللَّهِ أن يقولَ الرَّجلُ للرَّجلِ : اتَّقِ اللَّهَ ، فيقولُ عليكَ نفسَكَ

وَمَا خَلَقْتُ الْجِنَّ وَالْإِنسَ إِلَّا لِيَعْبُدُونِ