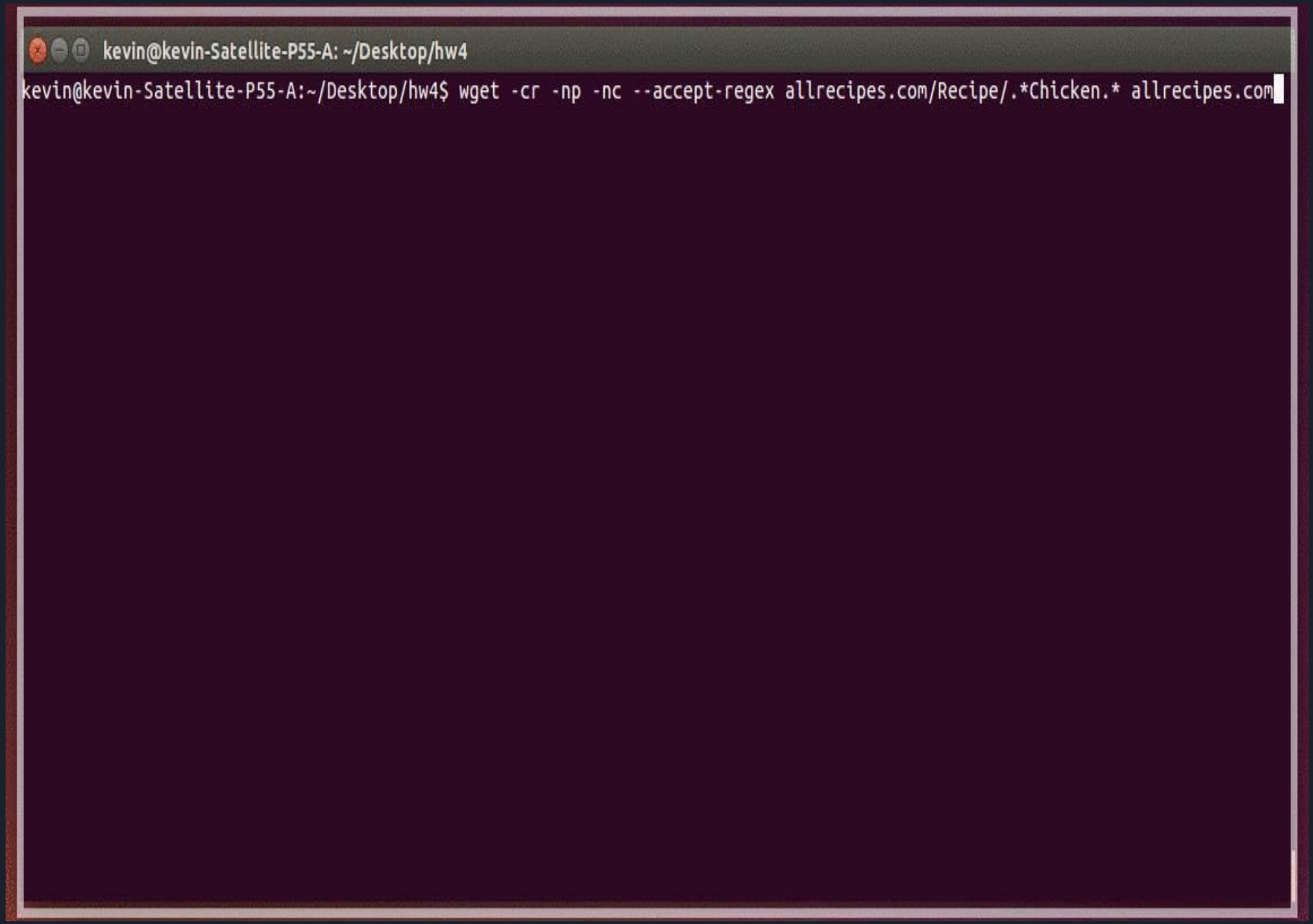
S.H.E.L.L.

SECURITY IS AN ILLUSION

S.H.E.L.L.

BASIC LINUX COMMANDS


kevin@kevin-Satellite-P55-A: ~/Desktop/hw4
kevin@kevin-Satellite-P55-A:~/Desktop/hw4$ wget -cr -np -nc --accept-regex allrecipes.com/Recipe/.*Chicken.* allrecipes.com

```
bp-columns.1.2.zip
carta pasante.docx
clonezilla-live-2.1.2-20-i686-pae.iso
Convocatoria-Sinergia2013_2014.pdf
cosmicbuddy-1.1.rc2-update-1.zip
devuelta.jpg
frisco-for-buddypress.1.6.13.zip
gparted-live-0.16.1-1-i486.iso
jDownloader
logo_big_1.5.png
nautiluspatch_v3.4.2-0ubuntu8-1_amd64.deb
orgullo.jpg
Presupuesto Yova Systems MG030713A CPU GAMER.pdf
prueba borrar.docx
Responsive Wordpress Templates
seafile-server_1.7.0_x86-64.tar.gz
Solicitud-Sinergia2013.pdf
time.png
webmin-1.630-minimal.tar.gz
wp-members-es_ES.po~
geppettvs@MONSTRUO:~/Downloads$ exit
exit
geppettvs@MONSTRUO:~$ ./tty2gif.py typing ttyrecord
geppettvs@MONSTRUO:~$
```

Linux

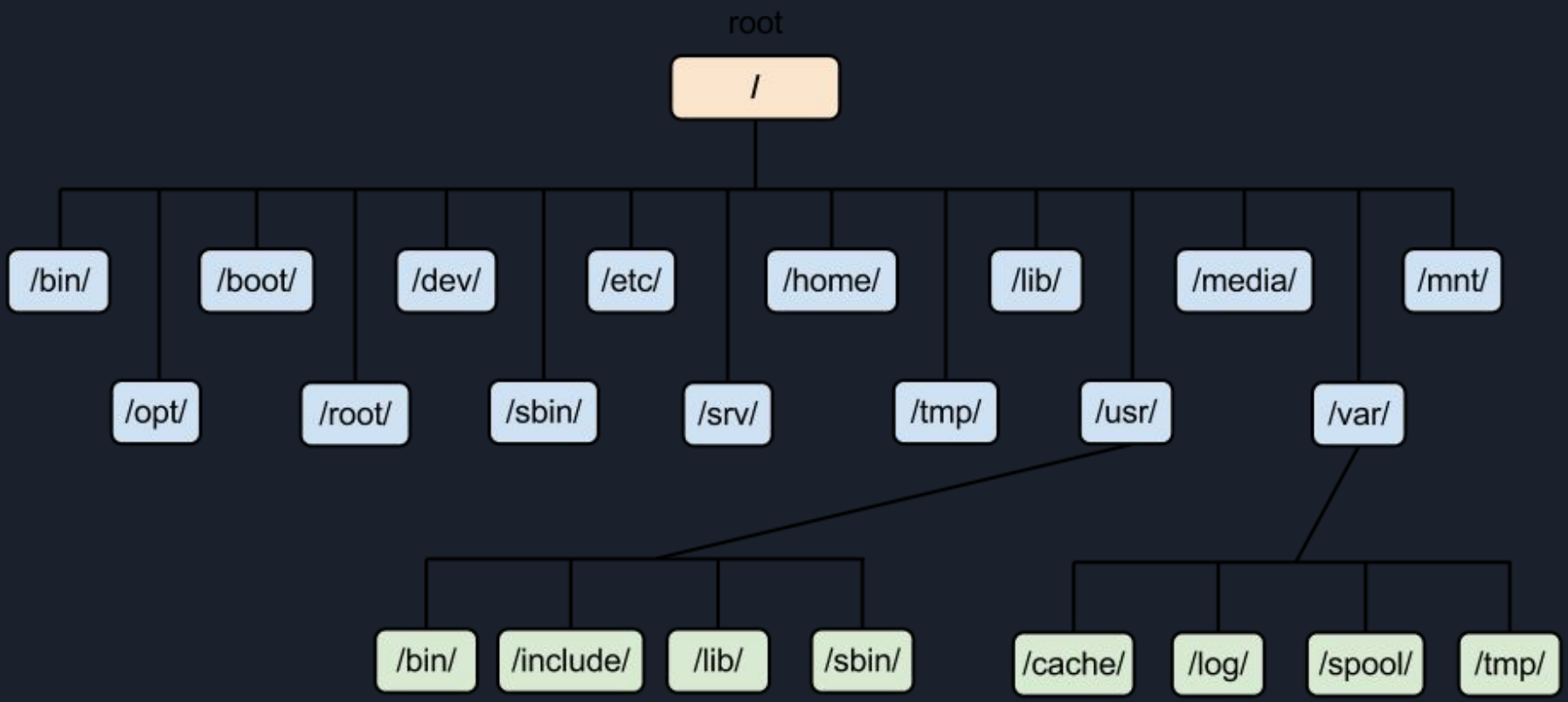
- Technically, GNU/Linux
- *GNU/Linux* is a family of open-source Unix-like operating systems based on the *Linux* kernel
- Open-source means software whose source code is publicly available, anyone can see, use and even modify the source code.
- That’s why it's free and compatible with a large range of hardware.
- https://github.com/torvalds/linux

Why Linux?

- Linux is extensively used in the tech industry.
- Almost every website, and servers are hosted on it due to its way lesser overhead.
- So, it's important to learn and understand it.

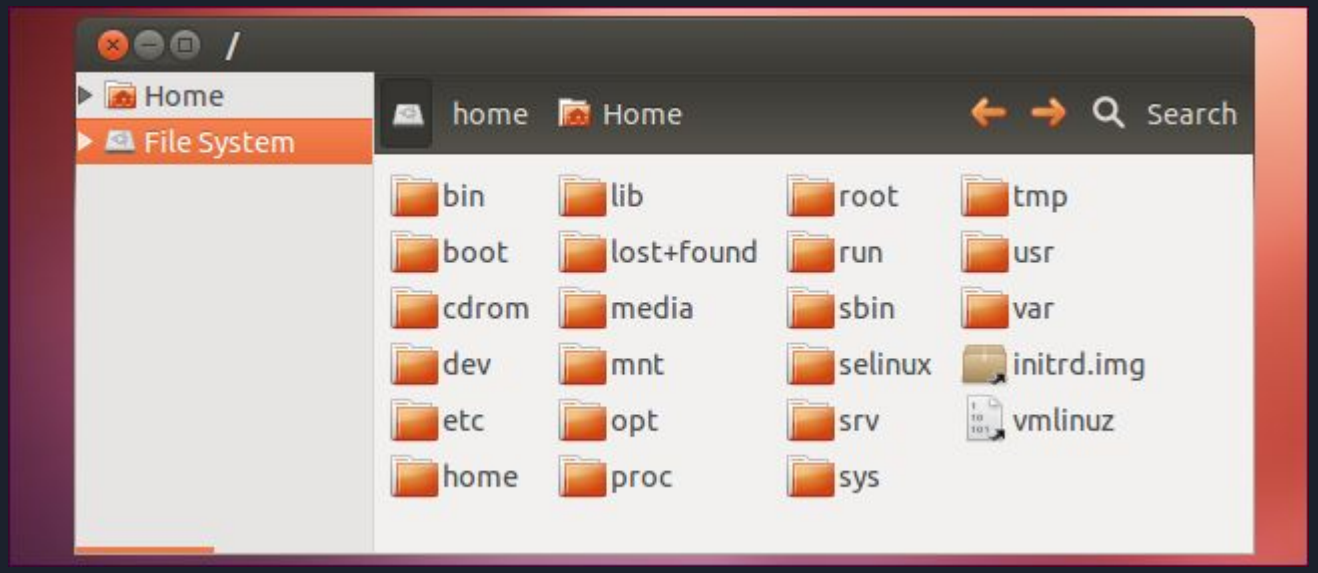
- Coming to why we use it for security, it's the safest operating system, with the least risk of malware(there will always be a risk) because the code is open source so patches can be applied quickly.
- Easier to manage software packages and tools.

File System in Linux



Directories

- Directories are nothing but “folders” as we call them in Windows.
- They contain the various files.
- The entire OS is organized into these directories.



The /bin directory contains the binaries and other executable programs. Most of the common Linux commands that we may as a user of the system are stored here.

The /boot directory contains the static boot loader files needed to boot the operating system

The /dev directory contains device files which are typically under the control of the operating system and the system administrators.

The /etc directory contains the system configuration files.

The /home directory contains a home directory for each user. Each user's personal files and user-specific configuration files are stored in their respective home directories

The /lib directory contains the essential system libraries and kernel modules which would be required by the binaries located under the /bin or /sbin directories

The /opt directory contains sub-directories for optional or third-party software.

The /proc directory contains information about the processes running on your system in directories named /proc/PID where PID is the process id.

The /usr directory is used to contain the applications and file pertaining to a particular user as compared to the files and applications of the system.

The /var directory is used to store the log files ,packages and databases.

Users and Groups

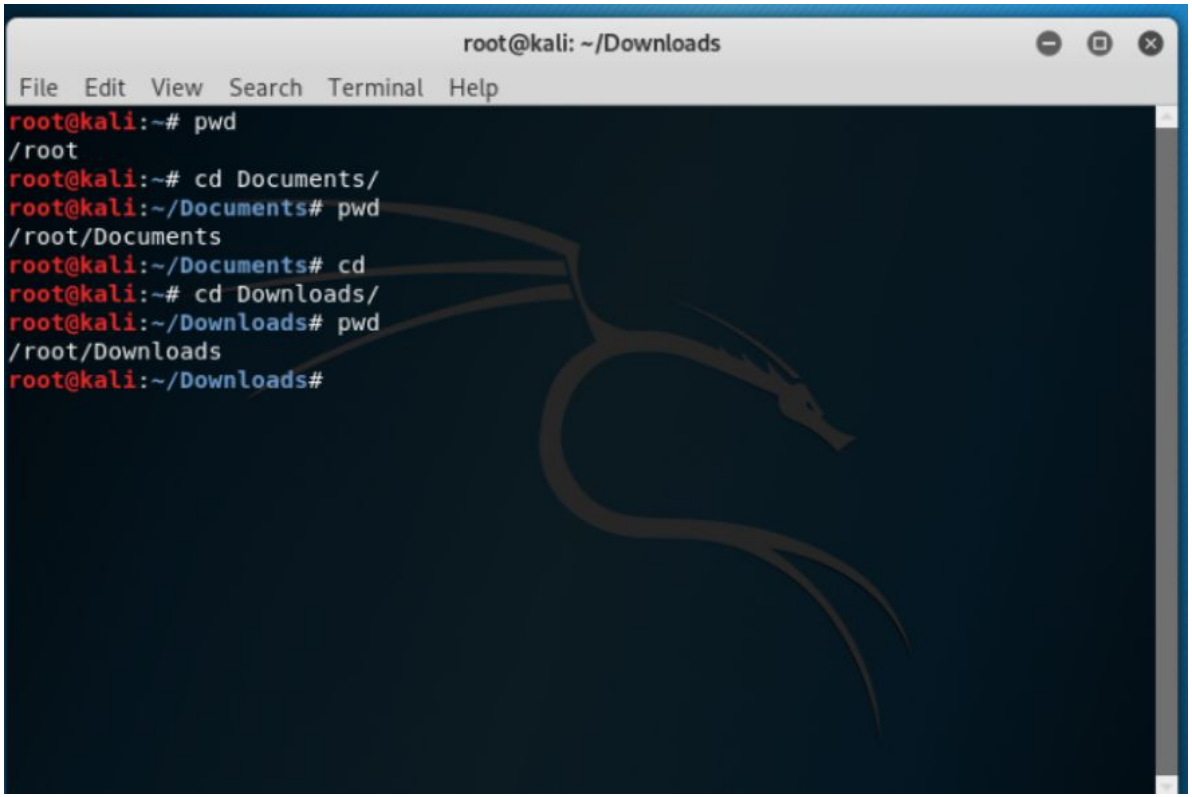
- Linux allows for multiple users to have interactive access to the system. Different users can have different permissions (privileges).
- The “root” user is the most-privileged user on the system. Same as “Administrator” in windows

- Groups are used to give a number of users (belonging to the same group) the same permissions.
- A user can be in multiple groups.

pwd

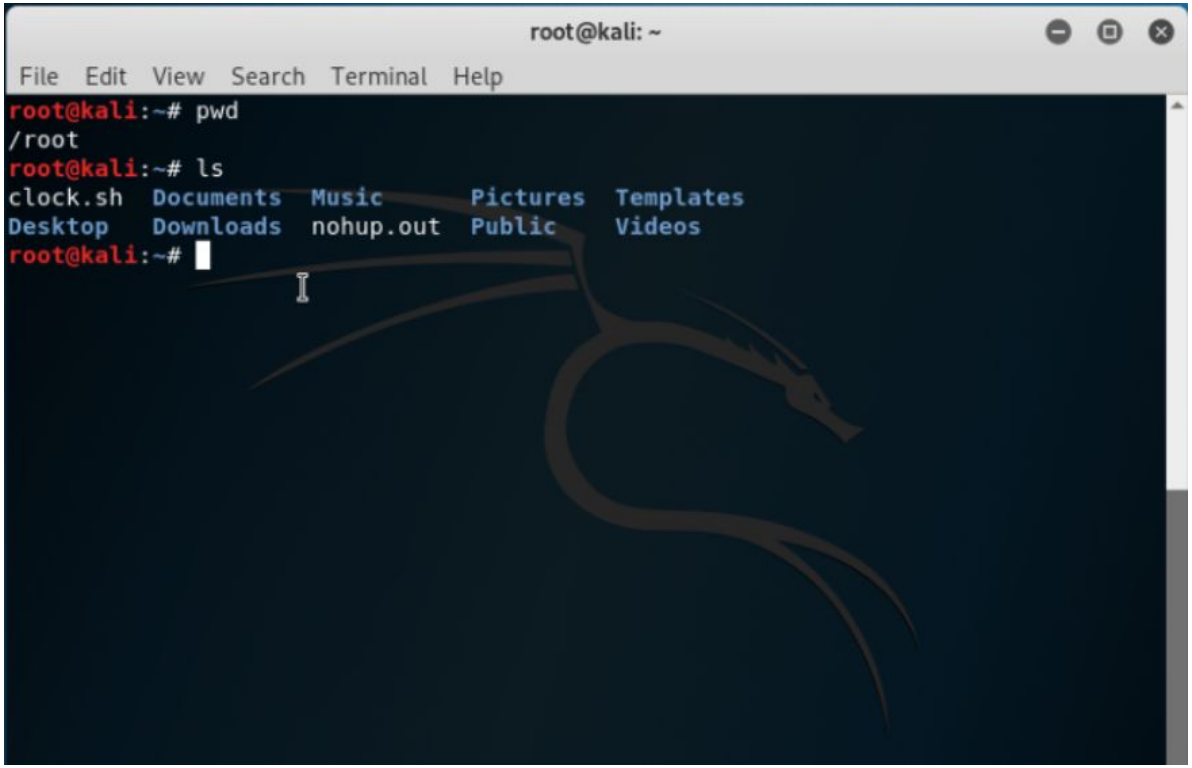
pwd means **Print Working Directory.**

This displays the current working directory.



ls

ls stands for ‘list’
ls is a command in linux which displays the list of files in the current working directory

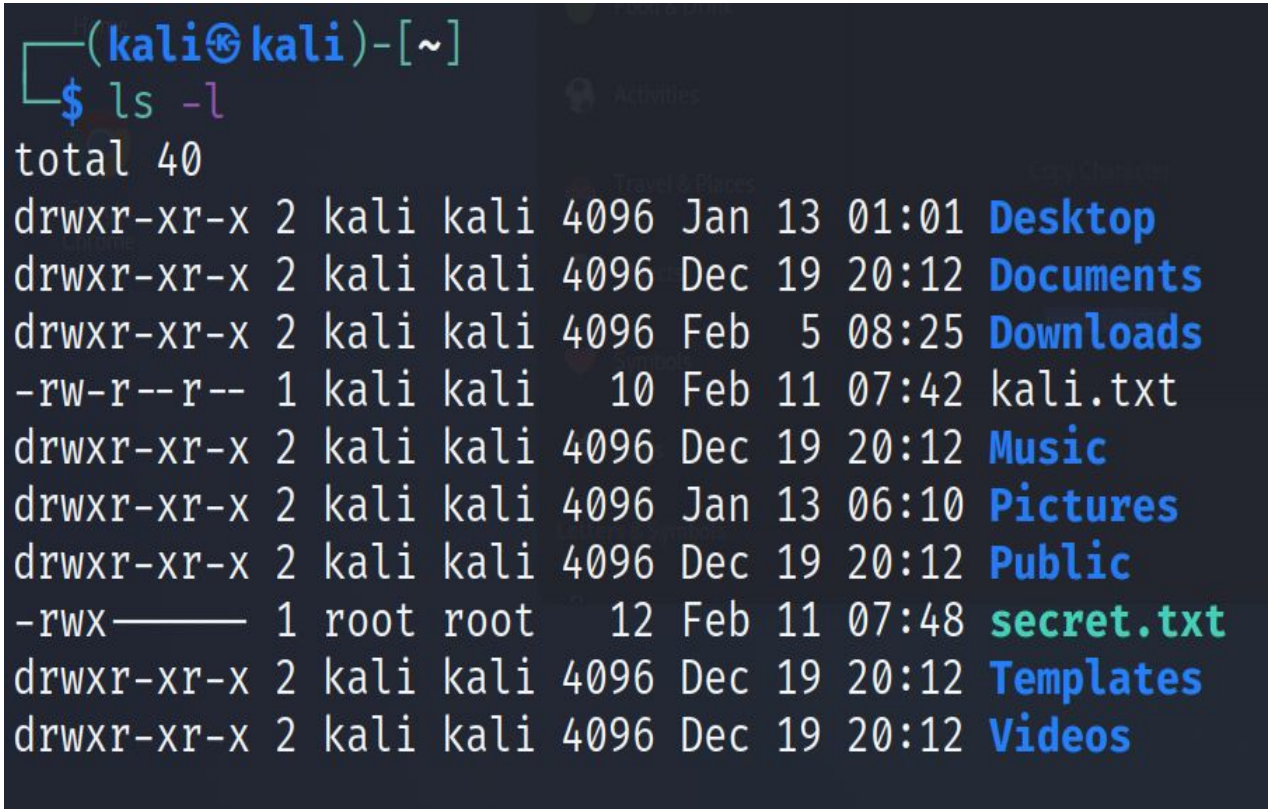


ls -l

-l stands for long listing

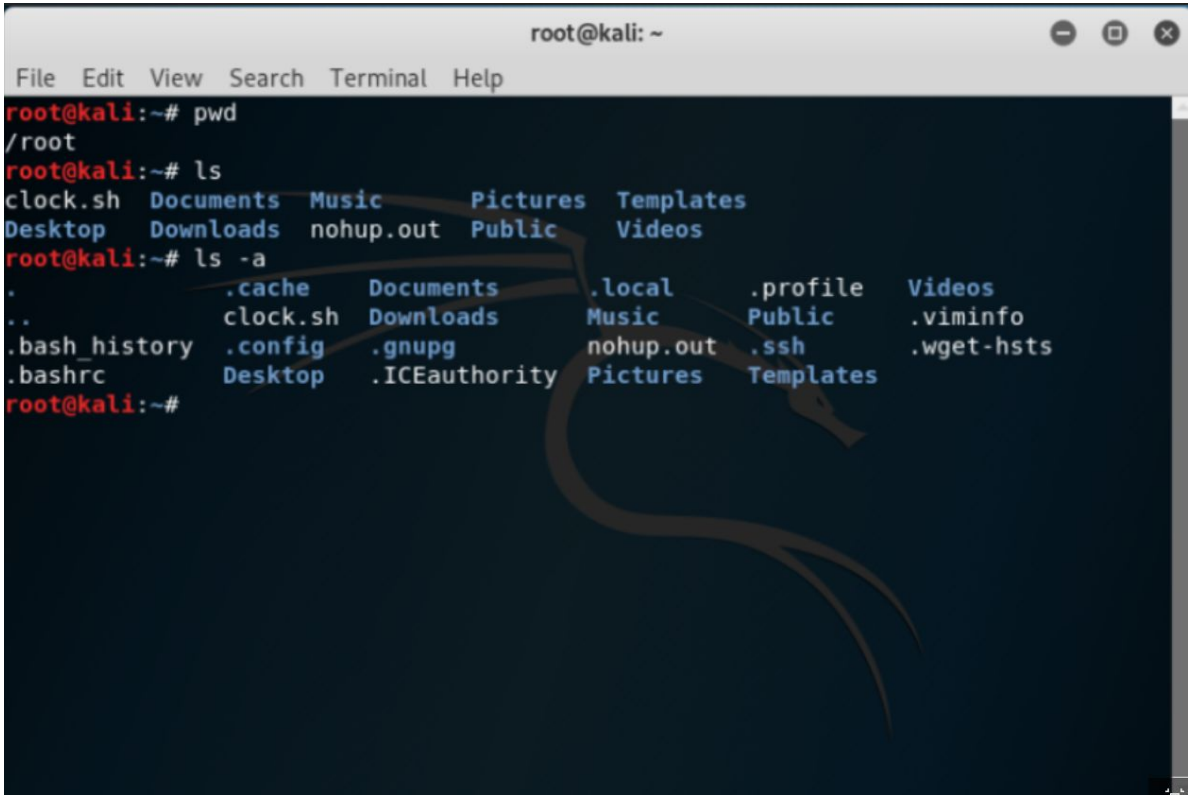
ls –l displays the file in long formats with its details.

Here the details mean the owner who created those files or directories and the date and time when the directory or file is created and the memory in bytes of the file or directory.



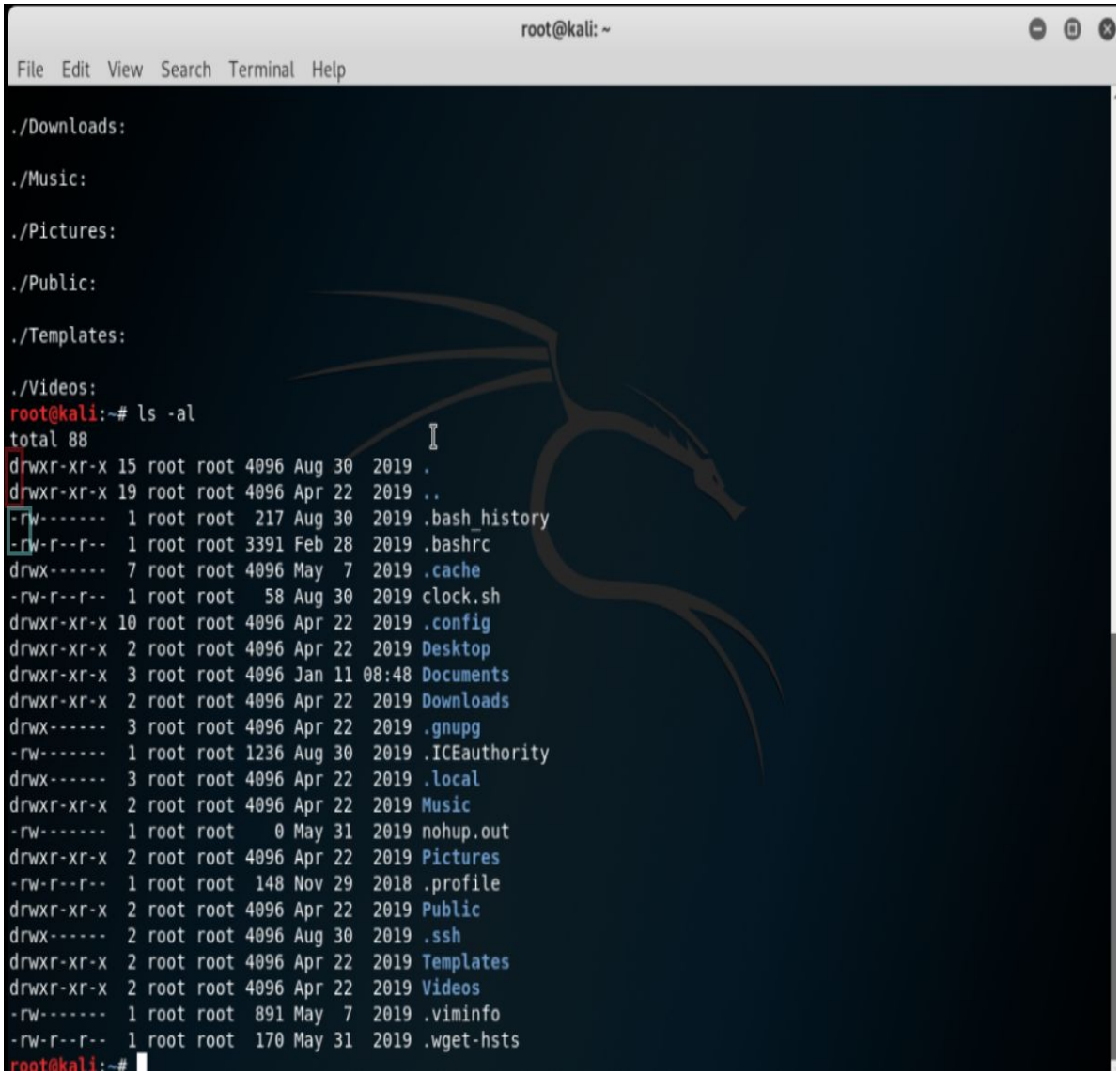
ls - a

'a' stands for 'all'
ls –a is a command in linux which displays the list of files including the hidden files in the current working directory.
Hidden files are files in linux which cannot be normally seen. They start with a dot (.). Such files won't be visible with ls but will be with ls -a



ls -al

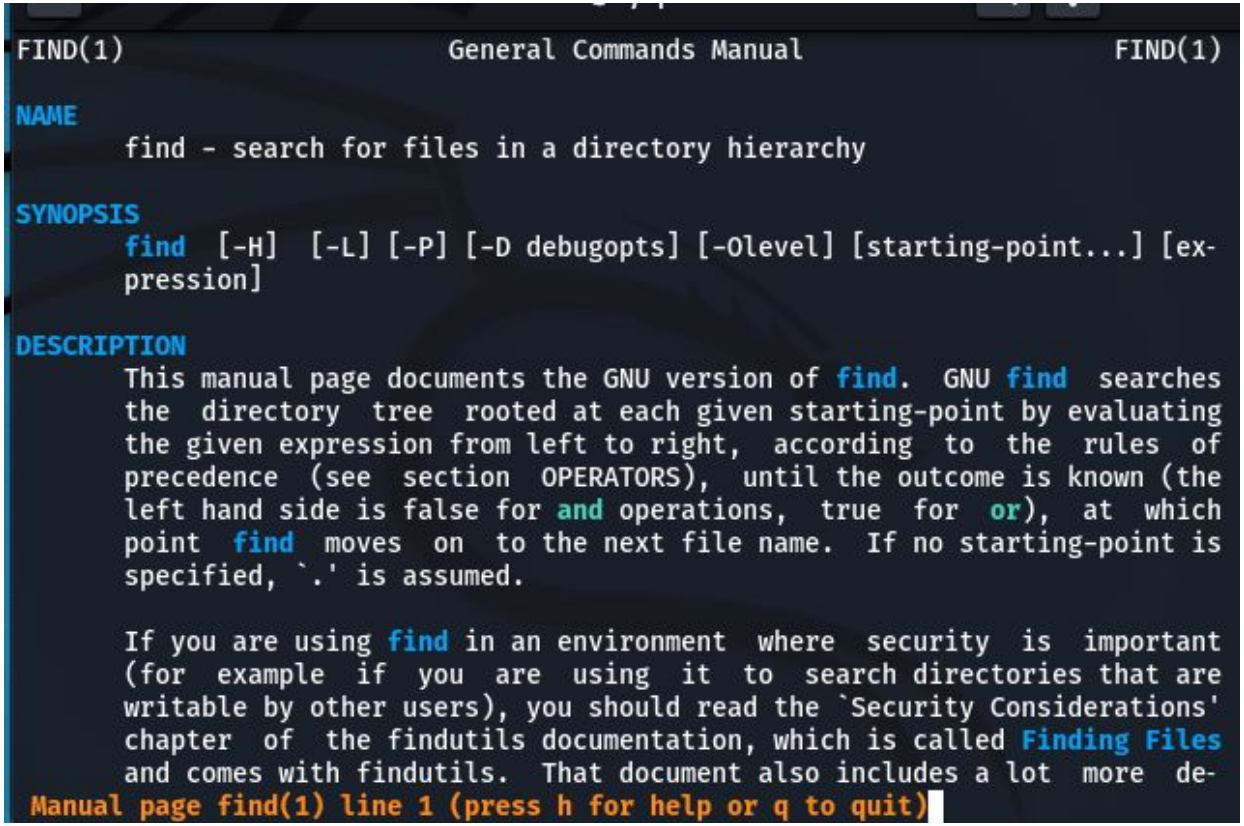
Parameters can also be combined.
ls –al is a combination of the two params, it will list all files/directories with details of the current working directory.



man

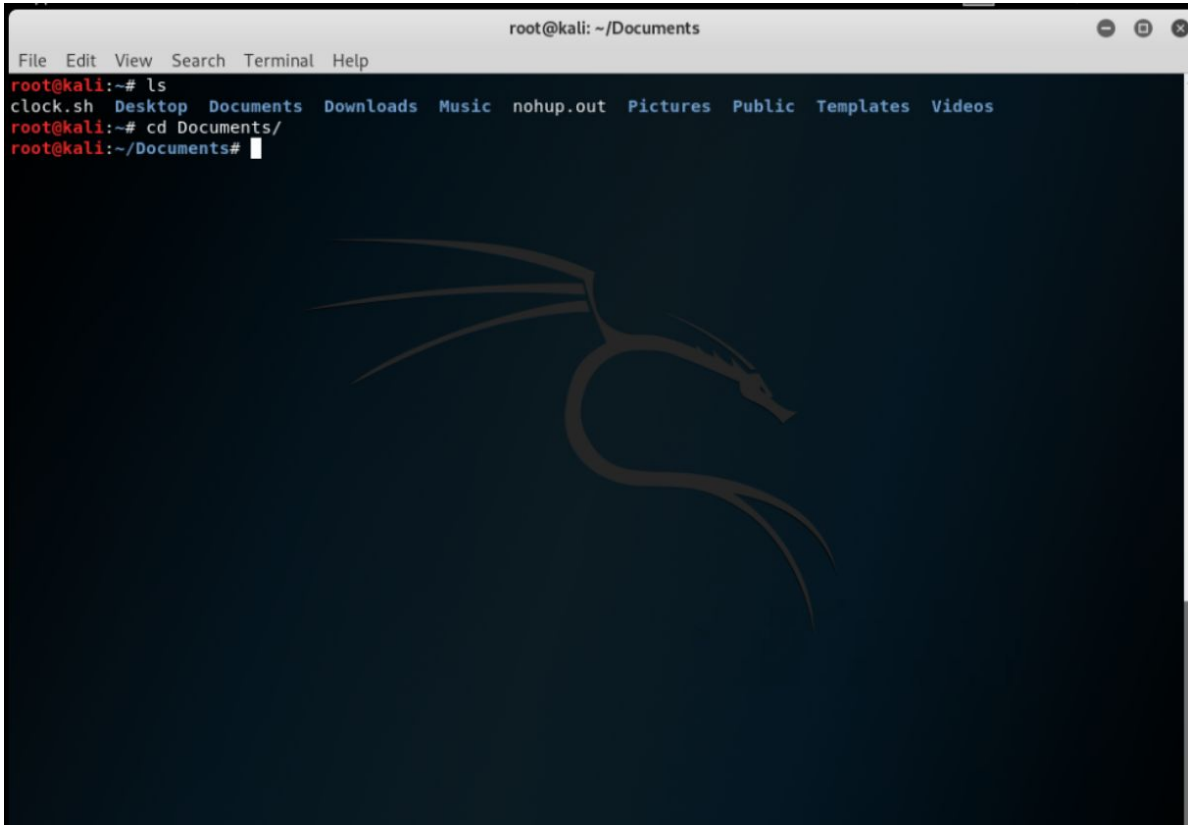
man stands for manual pages.

This command is used to get detailed information of other commands.



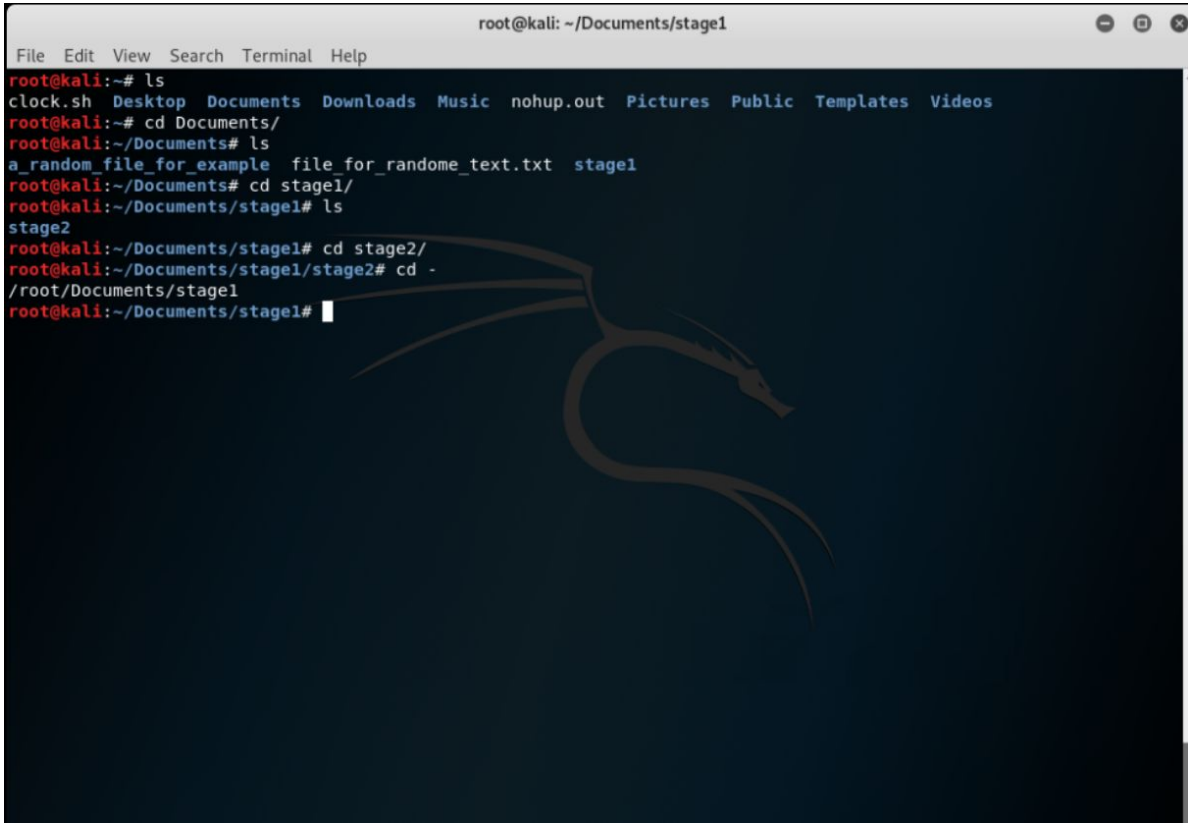
cd “dirname”

cd stands for ‘change directory’
cd is the command which is used for switching directories.



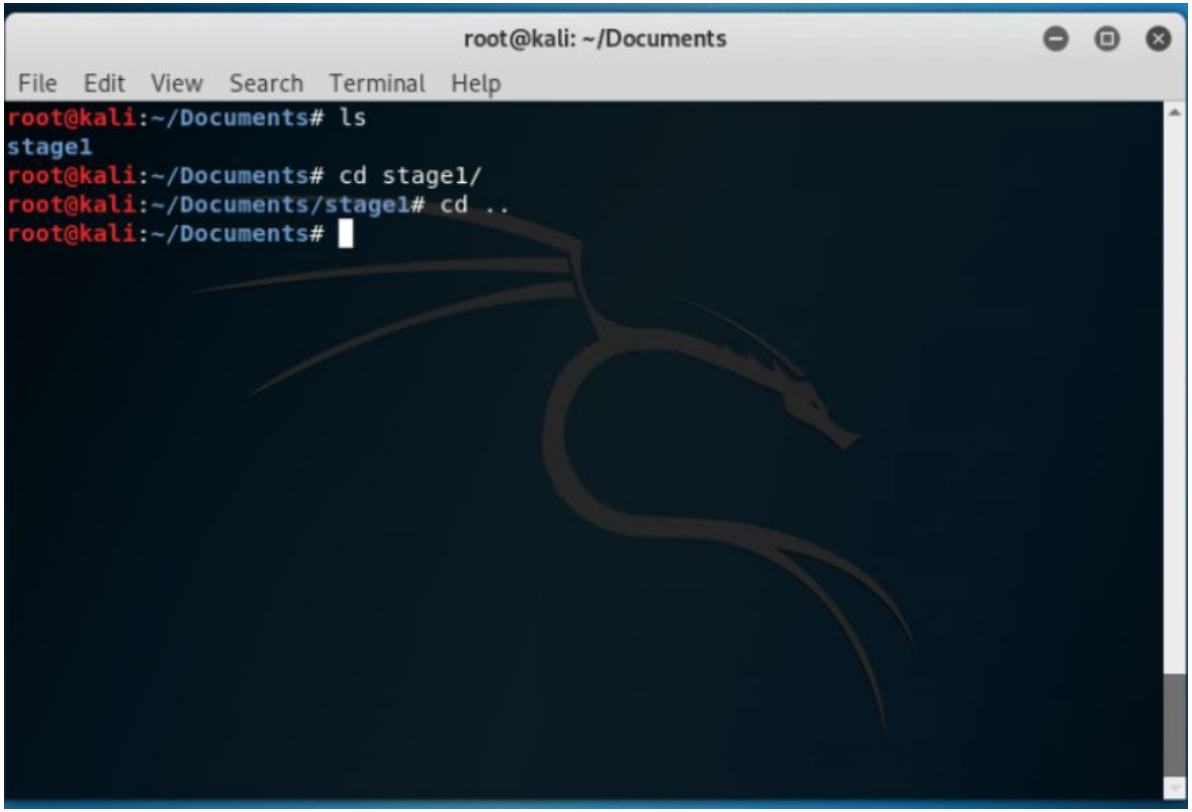
cd -

Here the extra - is used for switching back to the previous directory (before the last cd command) and displaying the current working directory .



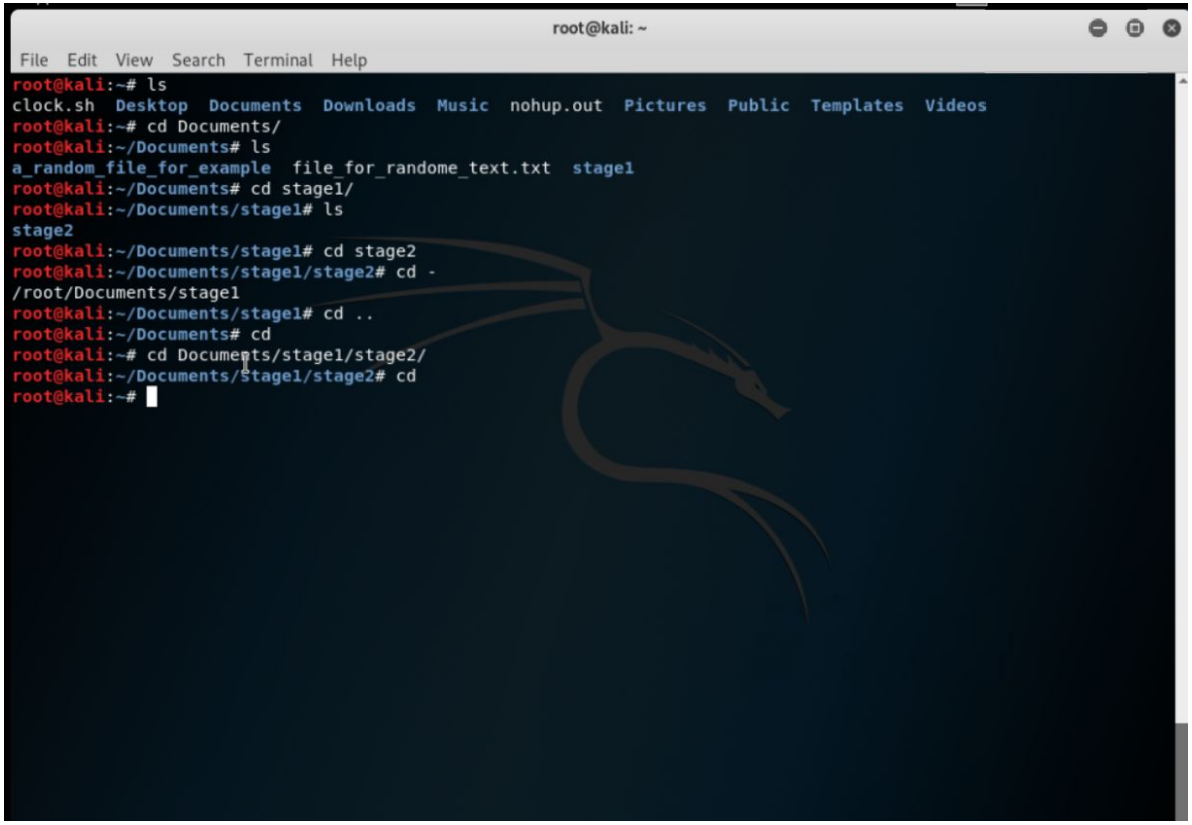
cd ..

cd .. takes you to the parent directory. (outer folder containing the current folder)



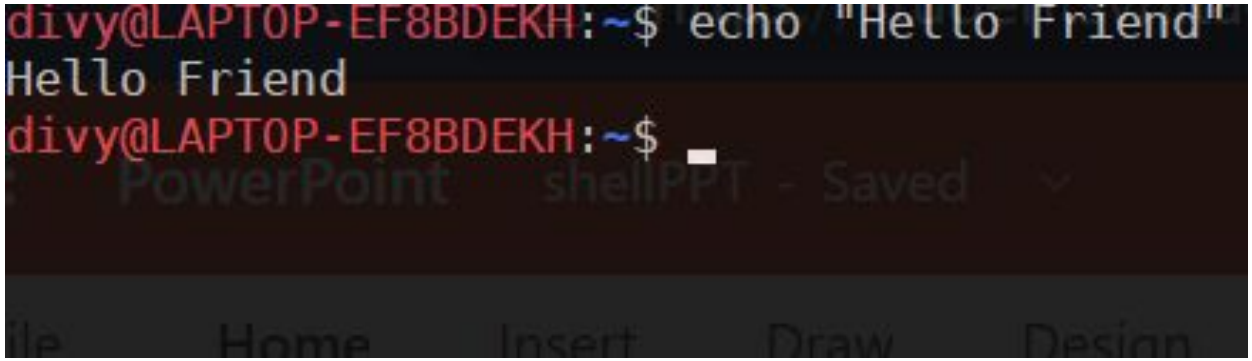
cd

In this case i.e. just cd without any file name after cd switches the current working directory with home directory.



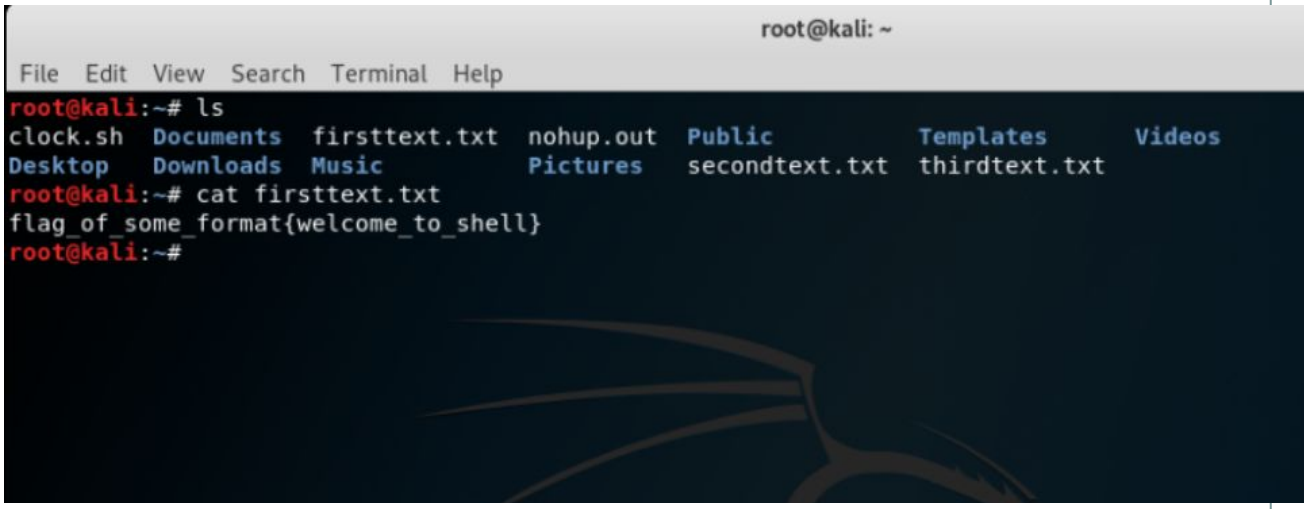
echo

Prints text to the console, enclosed in " "



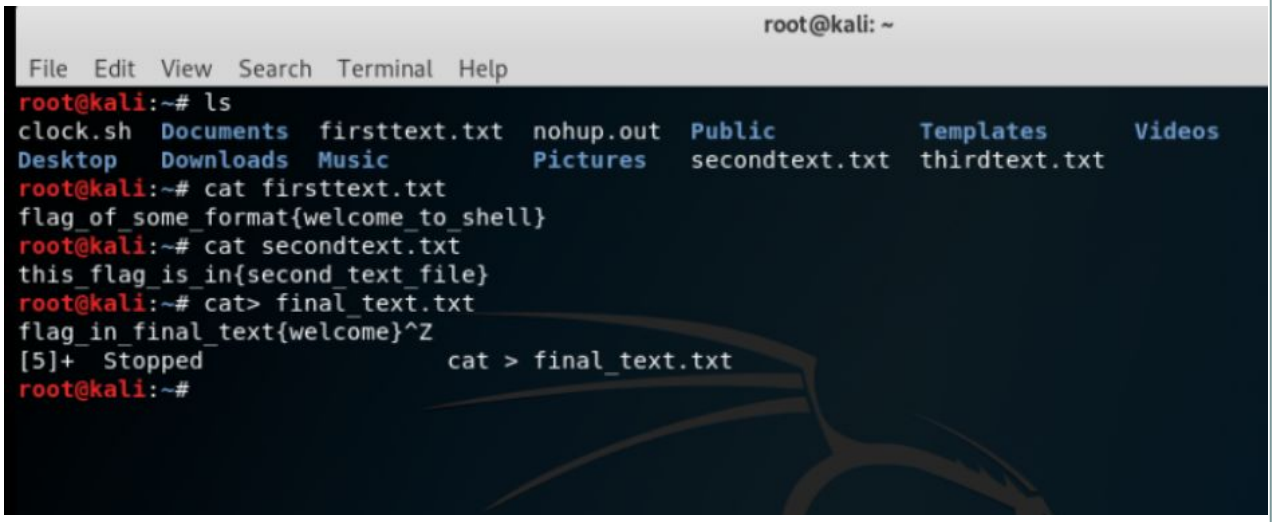
cat “file”

cat followed by file’s name displays the text in that file



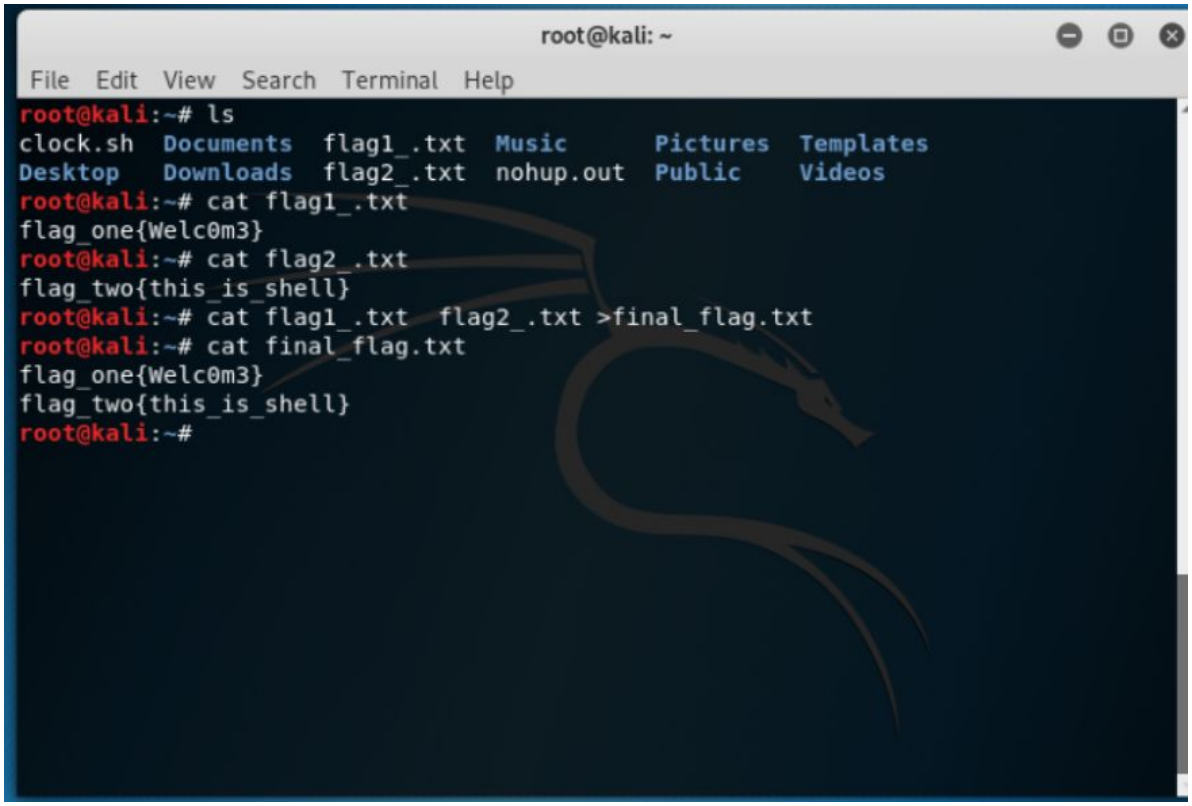
cat >newfile

This command creates a new file, and we can enter whatever text we want.



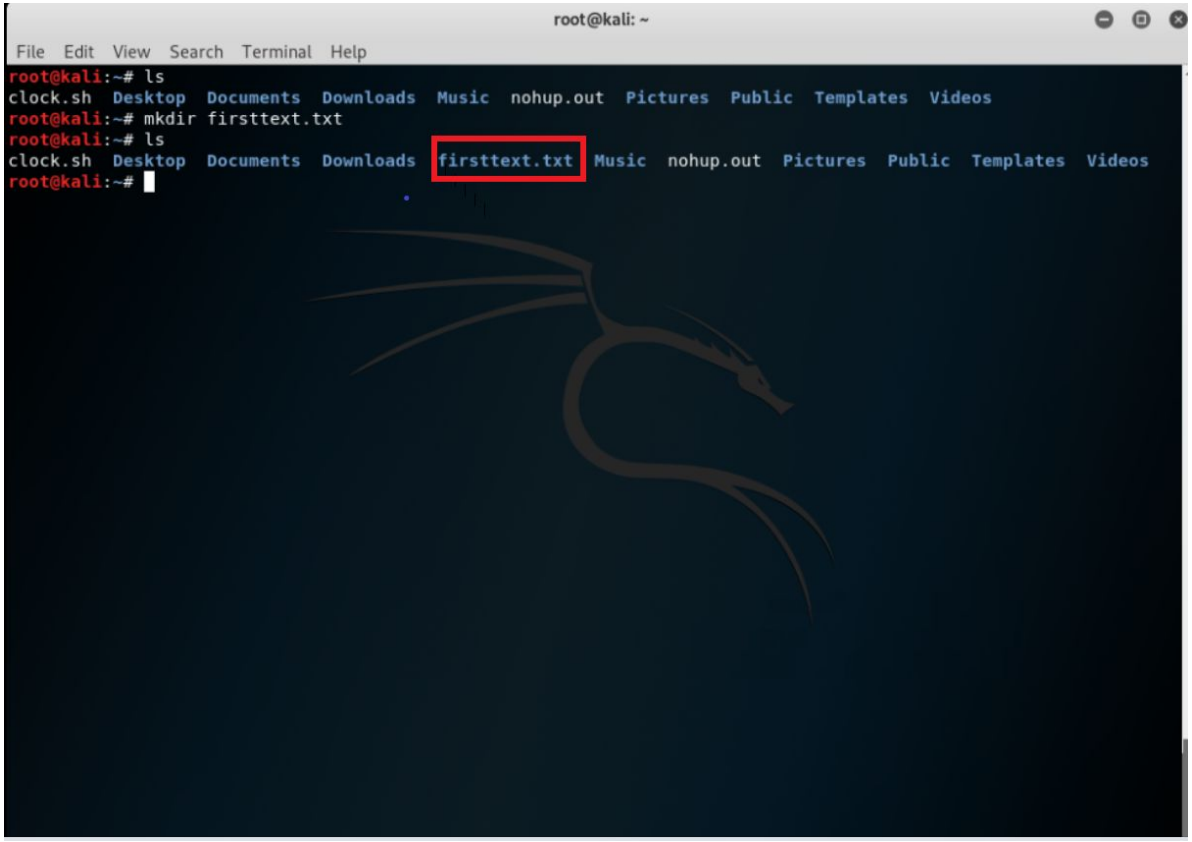
cat f1 f2 > f3

This command saves the text inside file f1 and f2 to file f3.



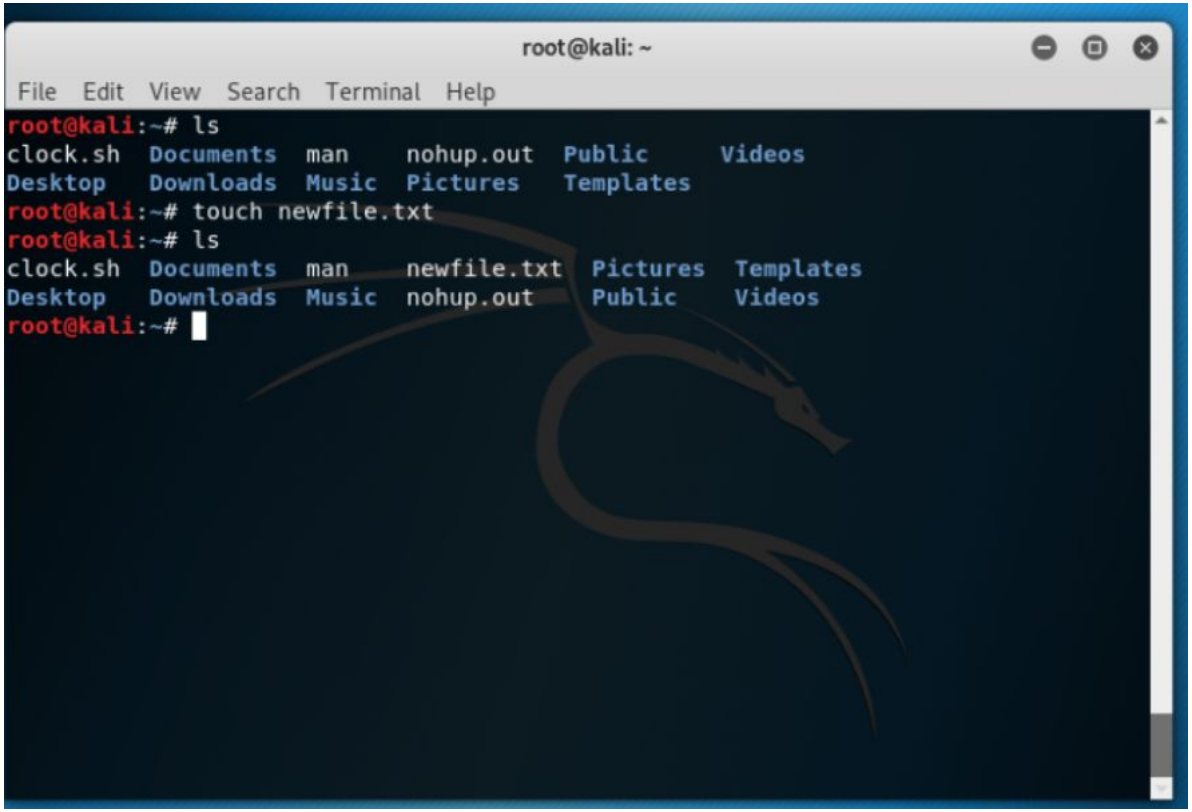
mkdir

This command is used to make directories.



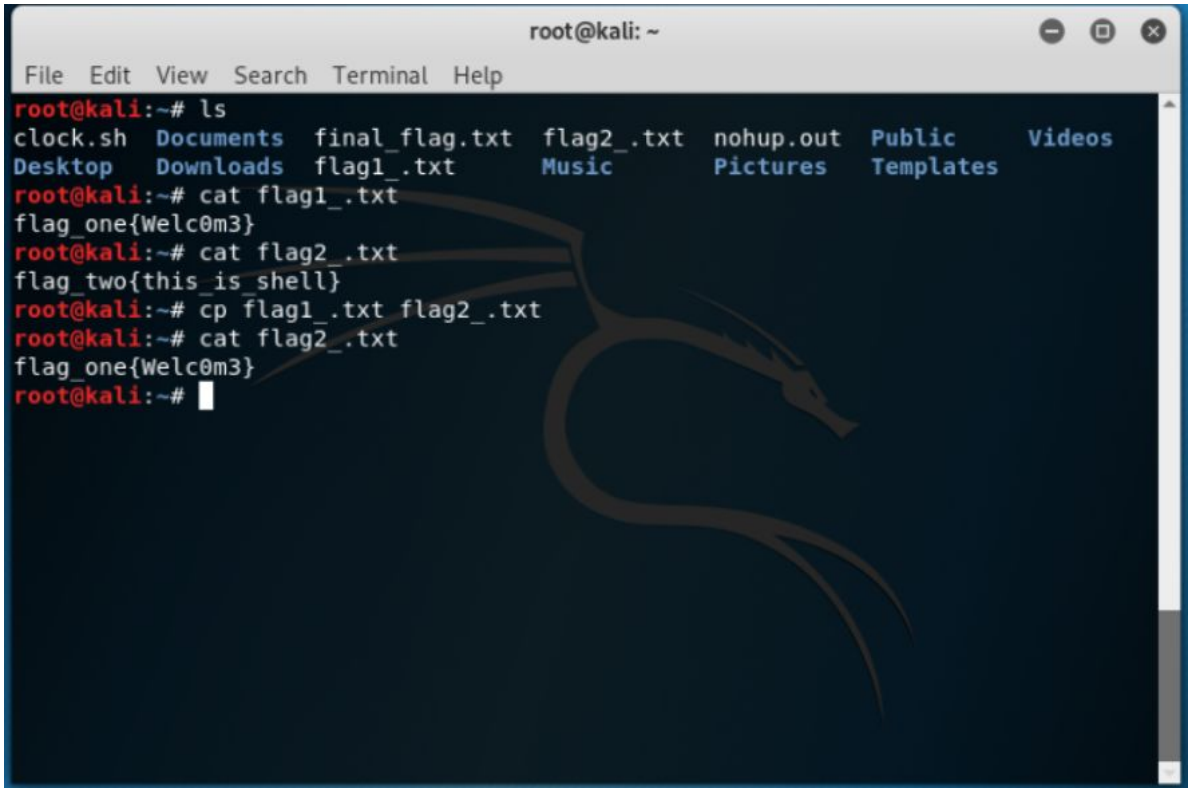
touch

This command allows you to create a blank new file through the linux command line.



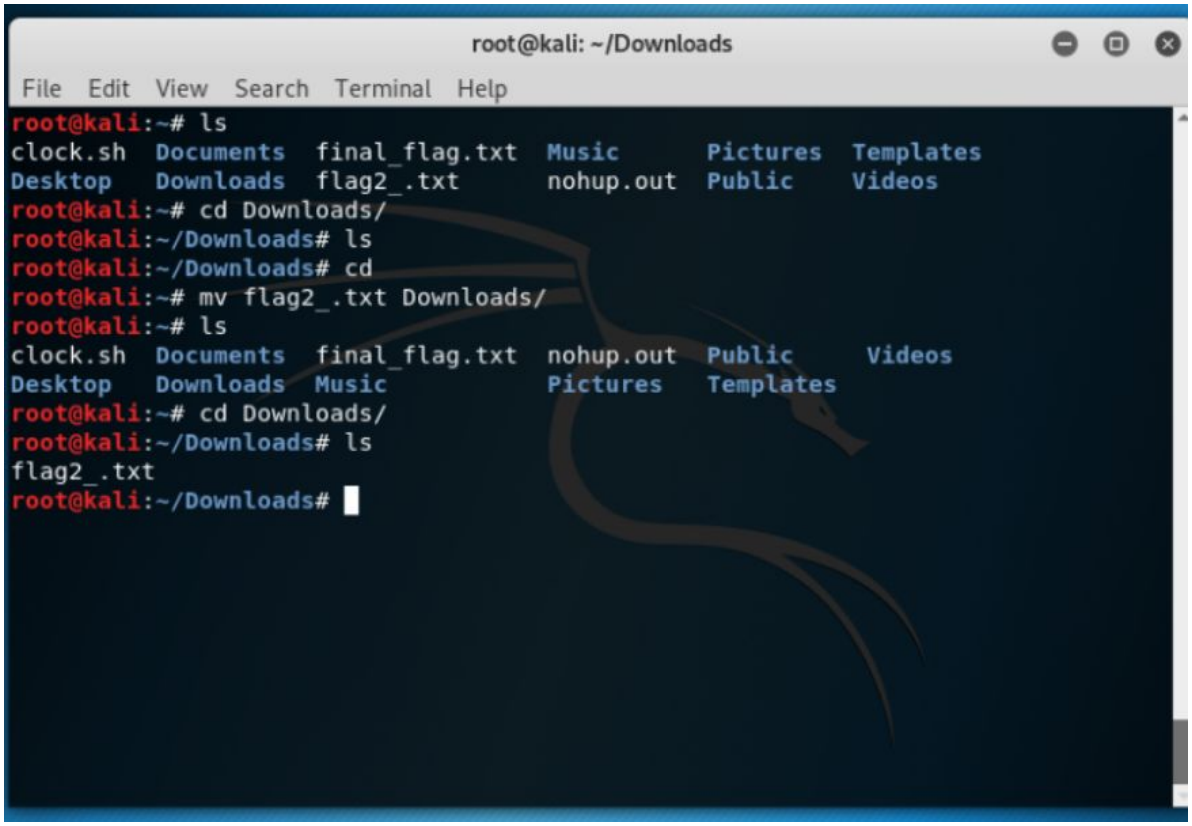
cp

This command is used to copy files from the any directory to any other directory.



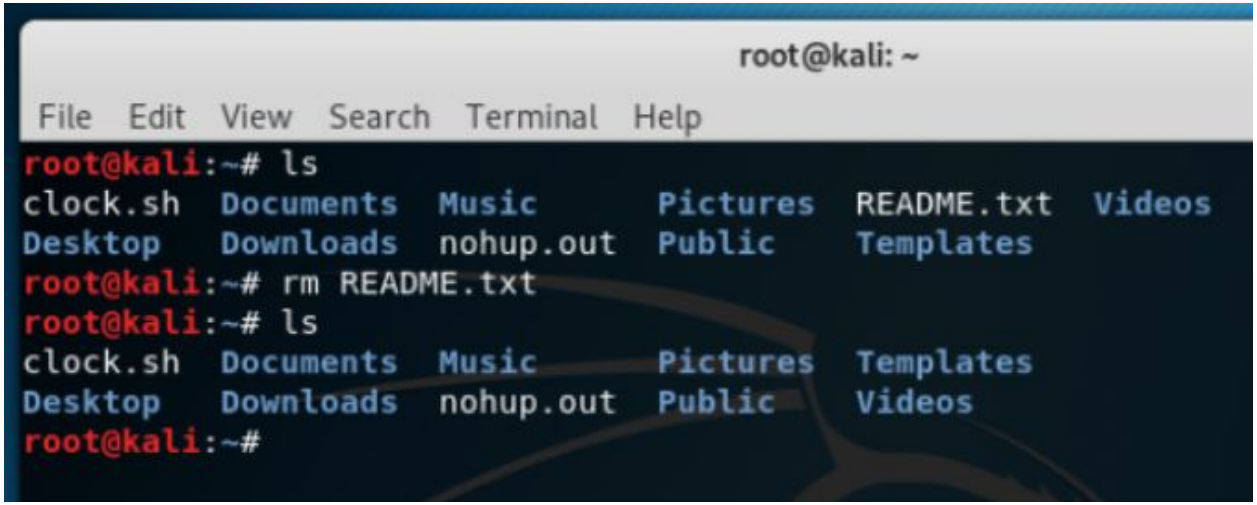
mv

This command is used for moving files or renaming files.



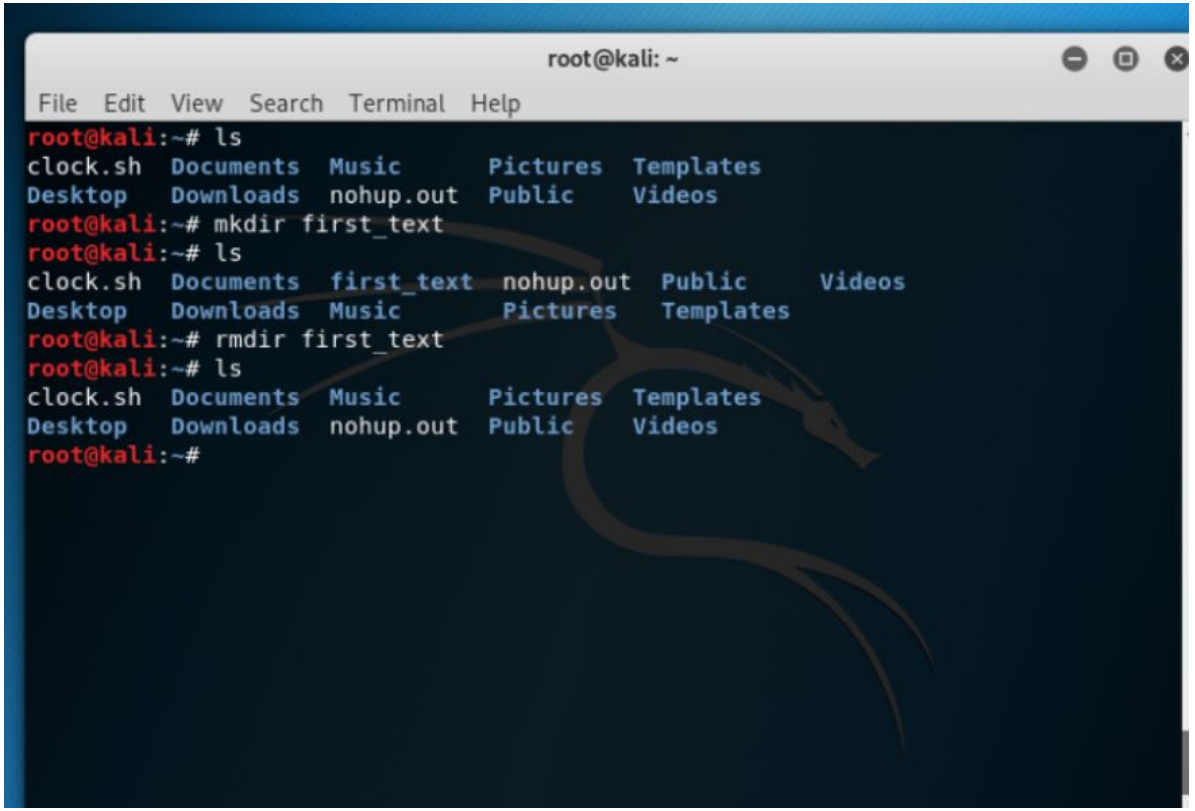
rm

This command is used to delete files.



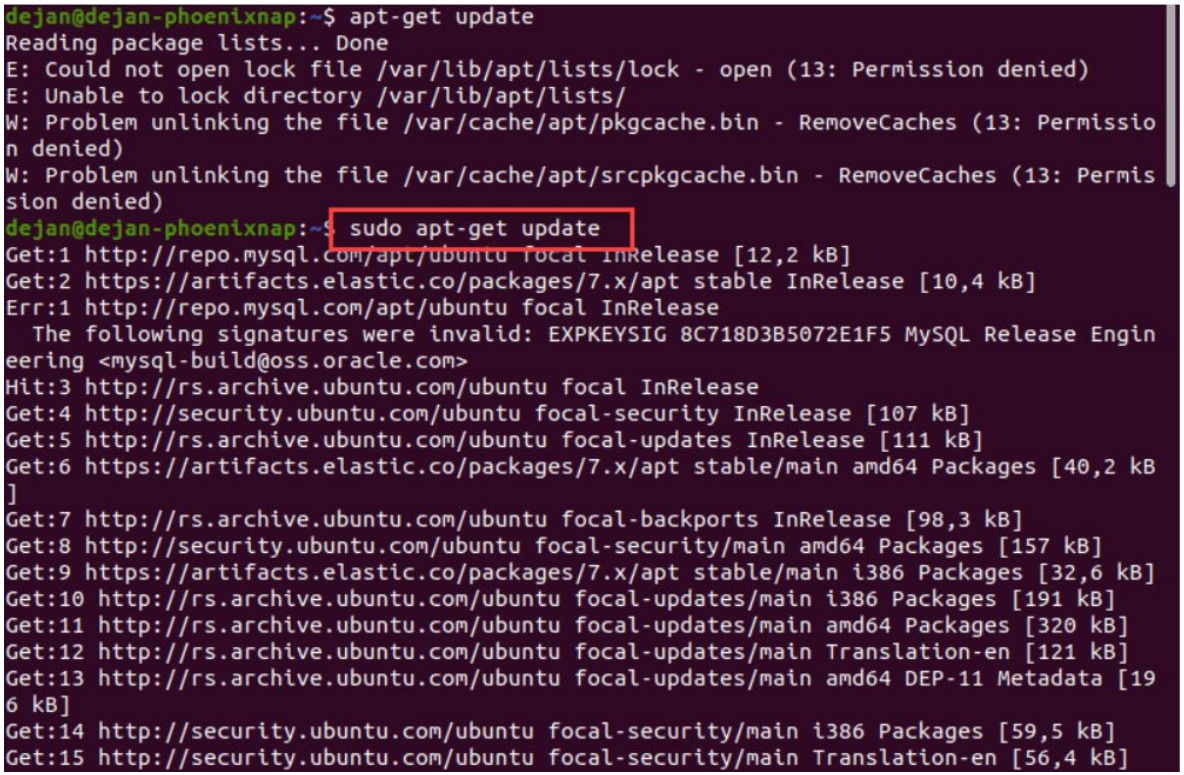
rmdir

This command is used to delete directories and the contents within them.



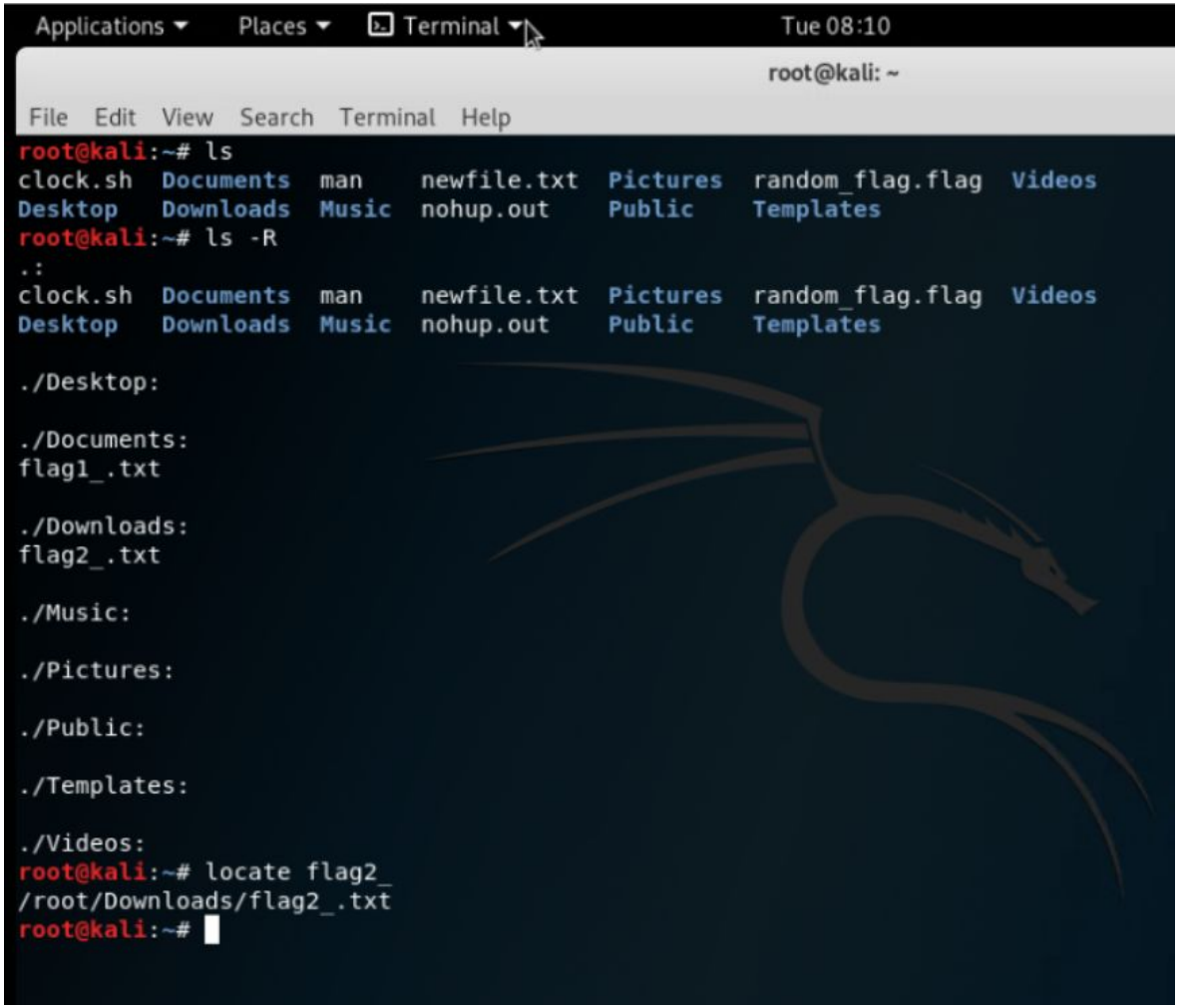
sudo

sudo (Super user do) enables you to perform tasks that require administrative or root permissions.



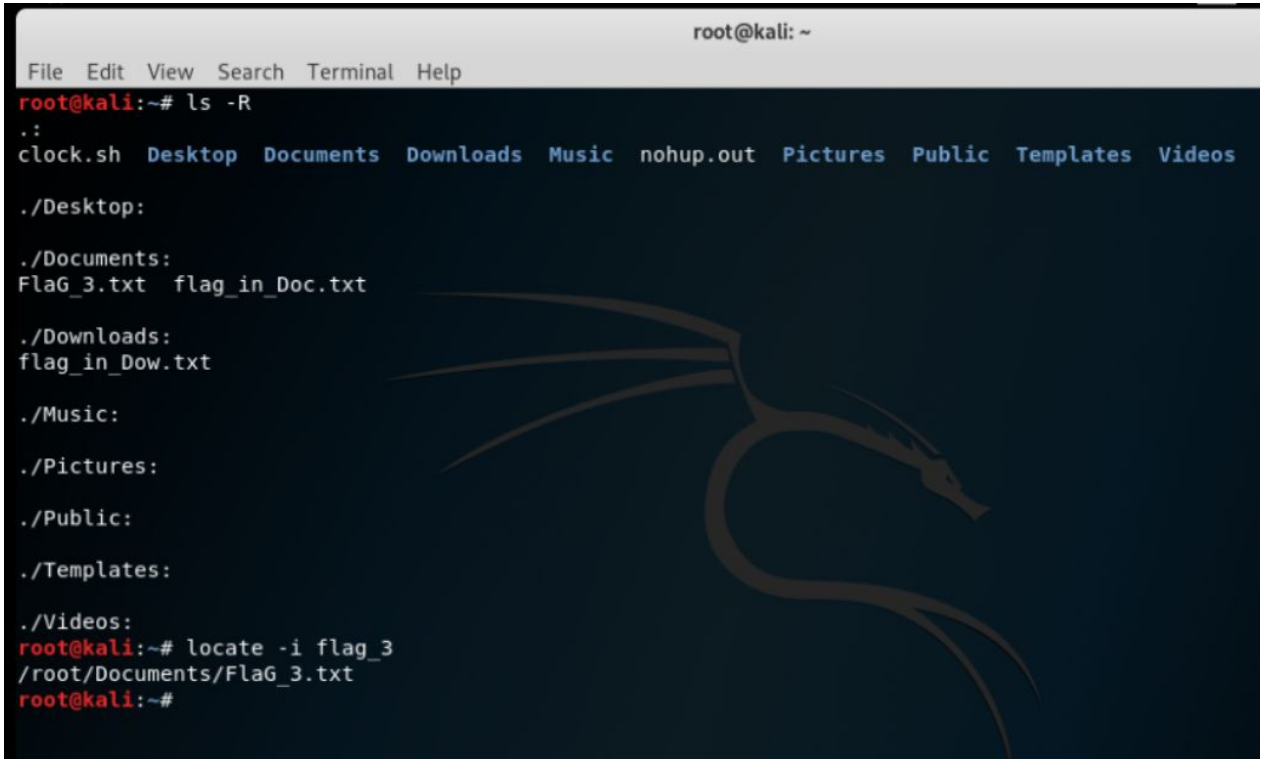
locate

This command is used to locate a file. (case sensitive)



locate -i

This command also serves the same purpose as of the command locate but it is case insensitive.



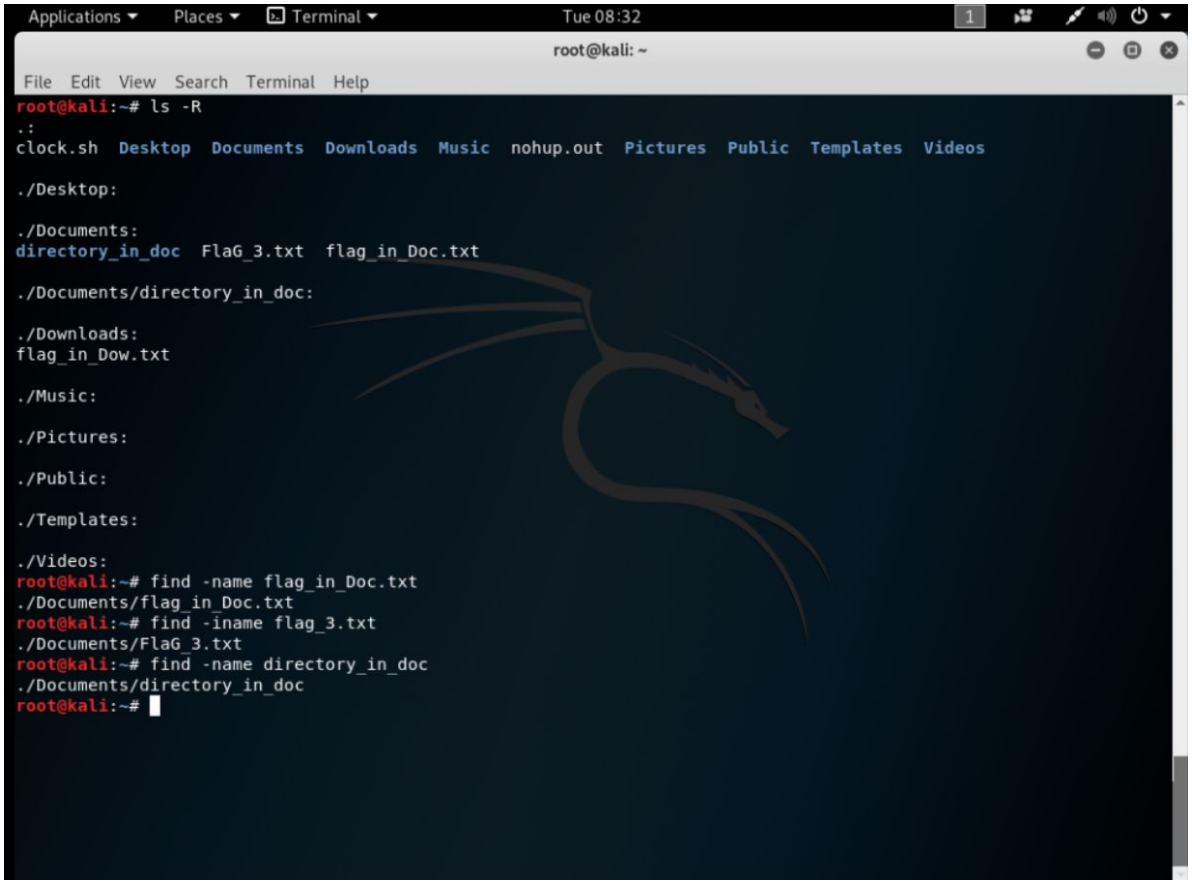
find

This command is similar to the command ‘locate’ this searches files and directories.

Here format is :

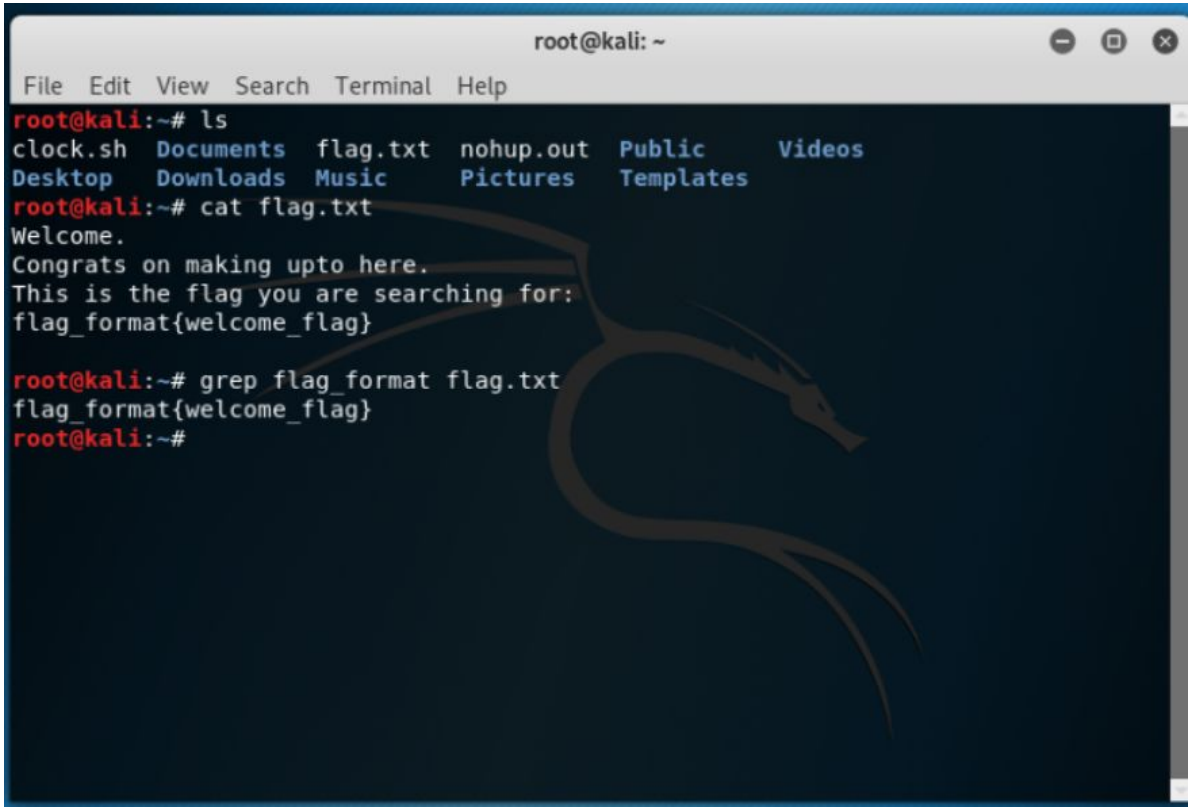
find –name “name of file/directory”

find –iname “name of file/directory for case insensitive”



grep

This command helps you to find a specific word in the whole text.



Permissions

Every file has three different permissions:

	numeric code
1. **read (r) -** can only view	4
2. **write (w) -** can view and edit	2
3. **execute (x) -** can execute if a program	1

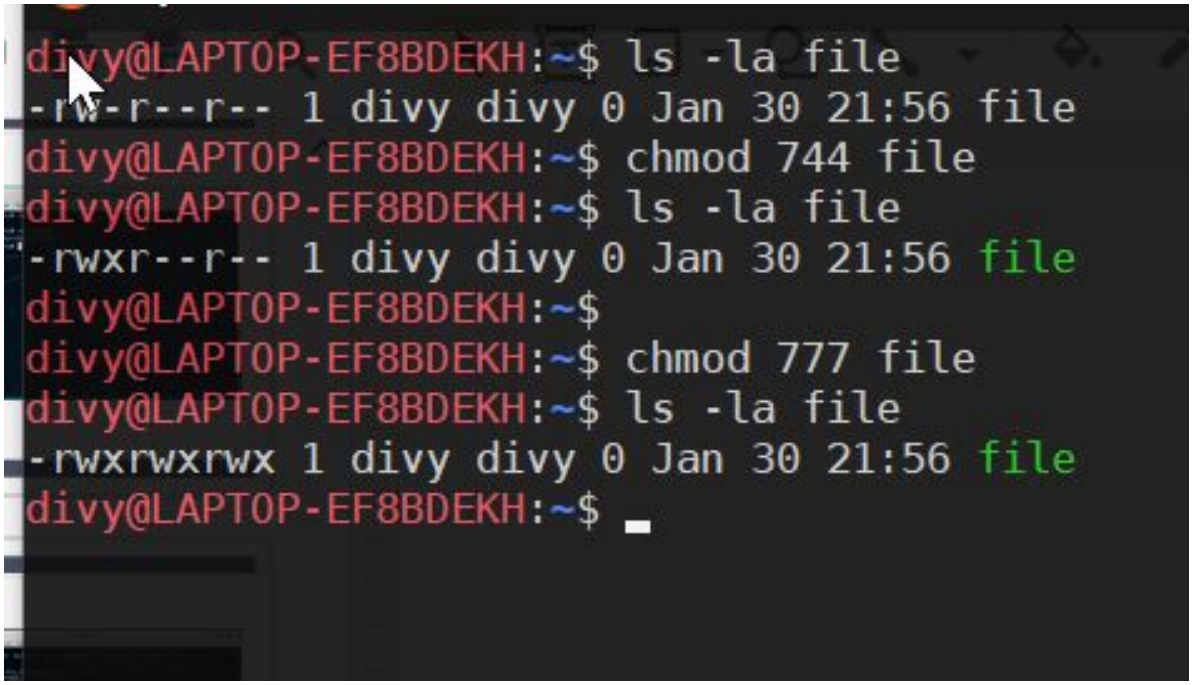
chmod

One can also use numeric codes to assign permissions.

chmod 744 file : 7 (4+2+1) for user and 4 and 4 for group and others.

(Put 0 for no permission)

chmod 777 file : makes the file fully accessible and executable

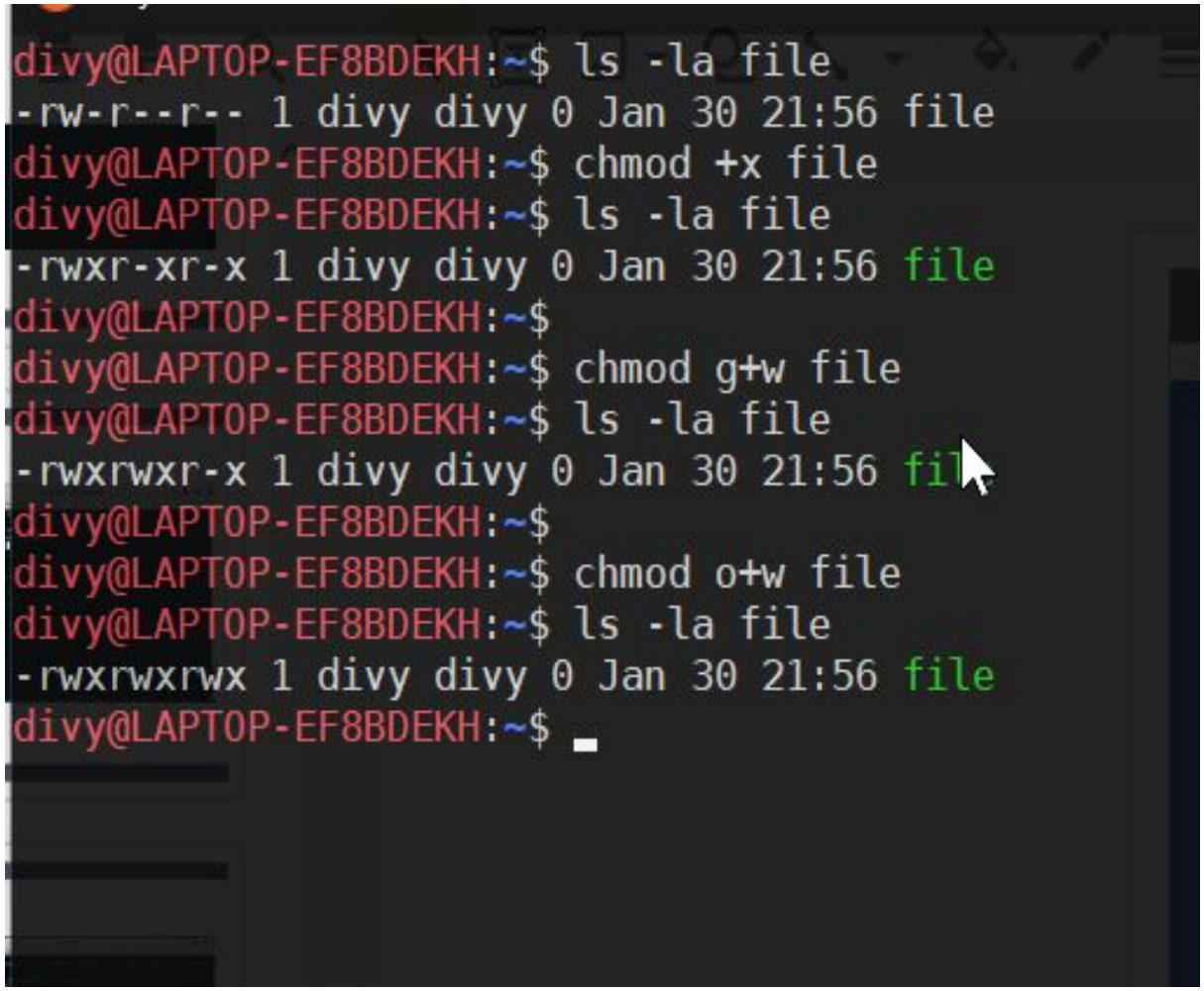


chmod

This is used to change the permissions of a file or a directory.

chmod +x file : every ownership exec permissions

if specific owership: then specify u, g or o with +x or +w



Your task for this week

Complete levels 1-10 of OverTheWire

https://overthewire.org/wargames/bandit/

Wargames Information updated

SSH Information
Host: bandit.labs.overthewire.org
Port: 2220

Bandit

Level 0
Level 0 → Level 1
Level 1 → Level 2
Level 2 → Level 3
Level 3 → Level 4
Level 4 → Level 5
Level 5 → Level 6
Level 6 → Level 7
Level 7 → Level 8
Level 8 → Level 9
Level 9 → Level 10
Level 10 → Level 11
Level 11 → Level 12
Level 12 → Level 13

Bandit

The Bandit wargame is aimed at absolute beginners. It will teach the basics needed to be able to play other wargames. **If you notice something essential is missing or have ideas for new levels, please let us know!**

Note for beginners

This game, like most other games, is organised in levels. You start at Level 0 and try to "beat" or "finish" it. Finishing a level results in information on how to start the next level. The pages on this website for "Level <X>" contain information on how to start level X from the previous level. E.g. The page for Level 1 has information on how to gain access from Level 0 to Level 1. All levels in this game have a page on this website, and they are all linked to from the sidemenu on the left of this page.

You will encounter many situations in which you have no idea what you are supposed to do. **Don't panic! Don't give up!** The purpose of this game is for you to learn the basics. Part of learning the basics, is reading a lot of new information.

There are several things you can try when you are unsure how to continue: