

Networking & System Administration Lab Record

Submitted To,
Ass prof. Meera Rose Mathew

Submitted By,
Nimisha James
RMCA-B S2
Roll No:11

TABLE OF CONTENT

EXP NO	EXPERIMENT	PAG NO
01	BASIC LINUX COMMANDS	03-64
02	NETWORK COMMANDS	65-83
03	LAMP INSTALLATION	84-88
04	ANSIBLE INSTALLATION	89-90
05	TCPDUMP INSTALLATION	91-92
06	SHELL SCRIPTING	93-102
07	WIRESHARK INSTALLATION	103-104
08	DOCKER INSTALLATION	105-110

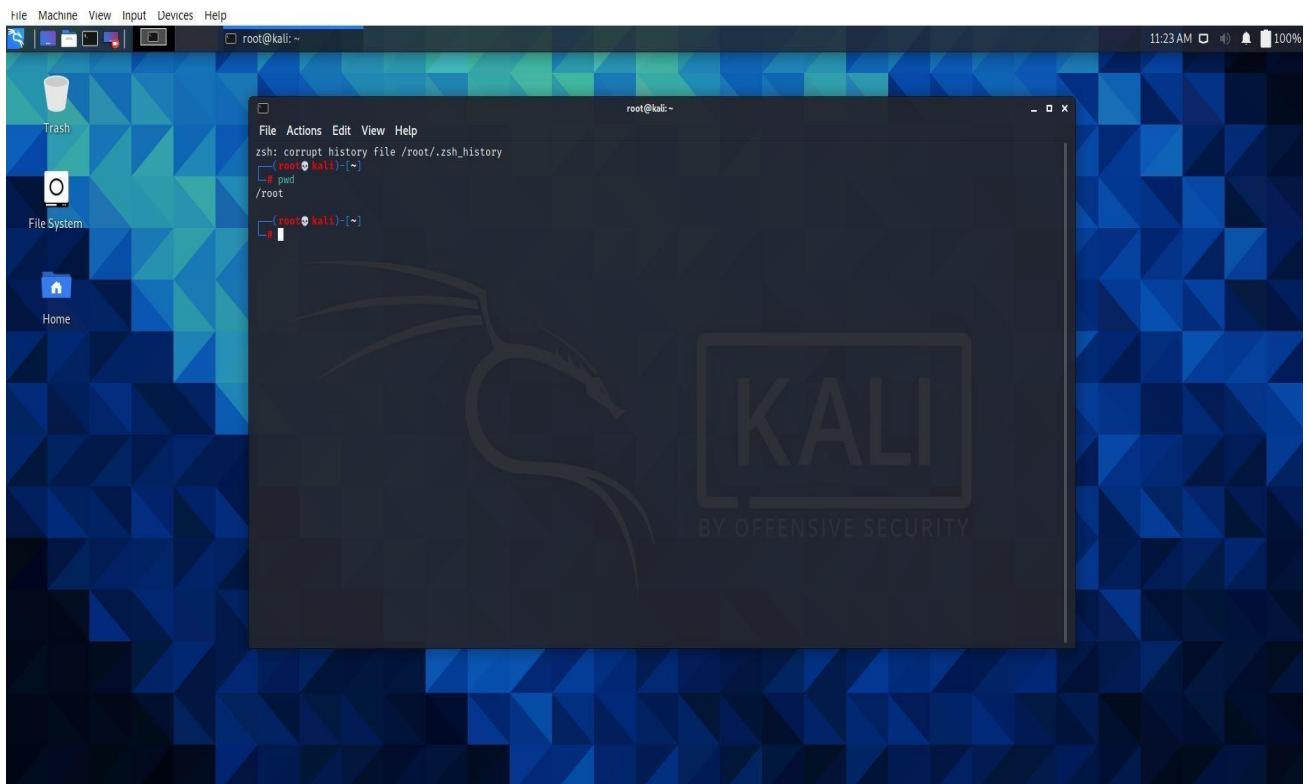
BASIC LINUX COMMANDS

pwd

pwd stands for **P**rint **W**orking **D**irectory. It prints the path of the working directory, starting from the root.

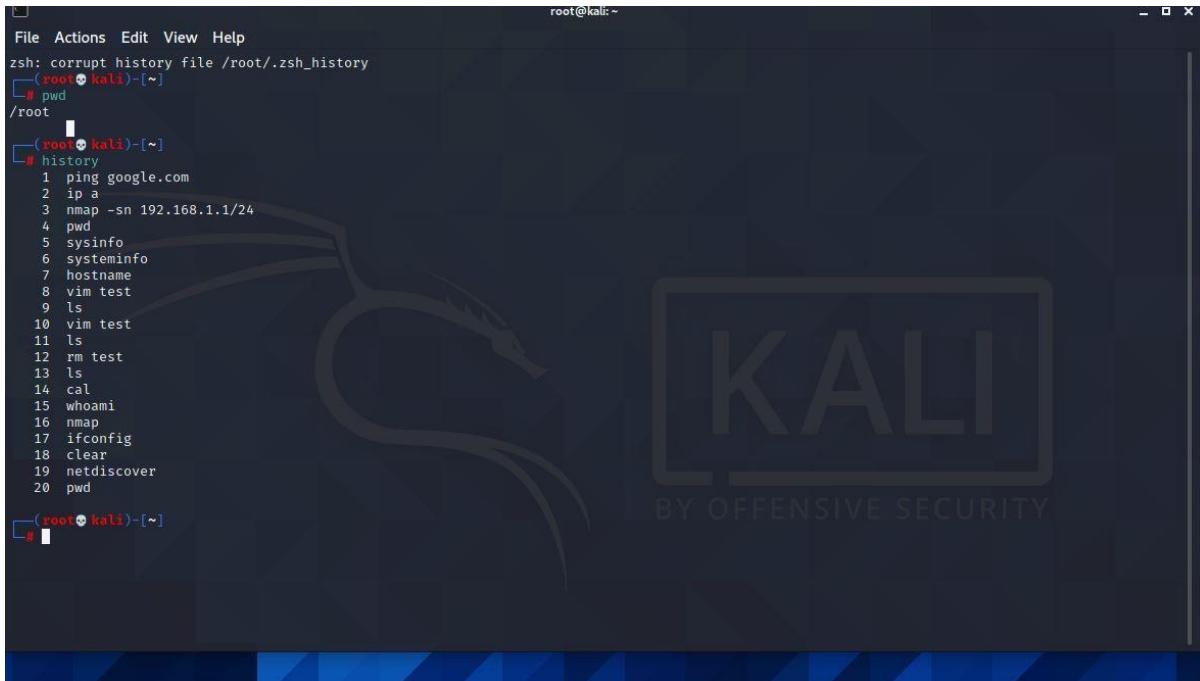
pwd is shell built-in command(**pwd**) or an actual binary(**/bin/pwd**).

\$PWD is an [environment variable](#) which stores the path of the current directory.



history

history command is used to view the previously executed command. This feature was not available in the Bourne shell. Bash and Korn support this feature in which every command executed is treated as the event and is associated with an event number using which they can be recalled and changed if required. These commands are saved in a history file. In Bash shell history command shows the whole list of the command.



The screenshot shows a terminal window titled "root@kali: ~". The window contains the following text:

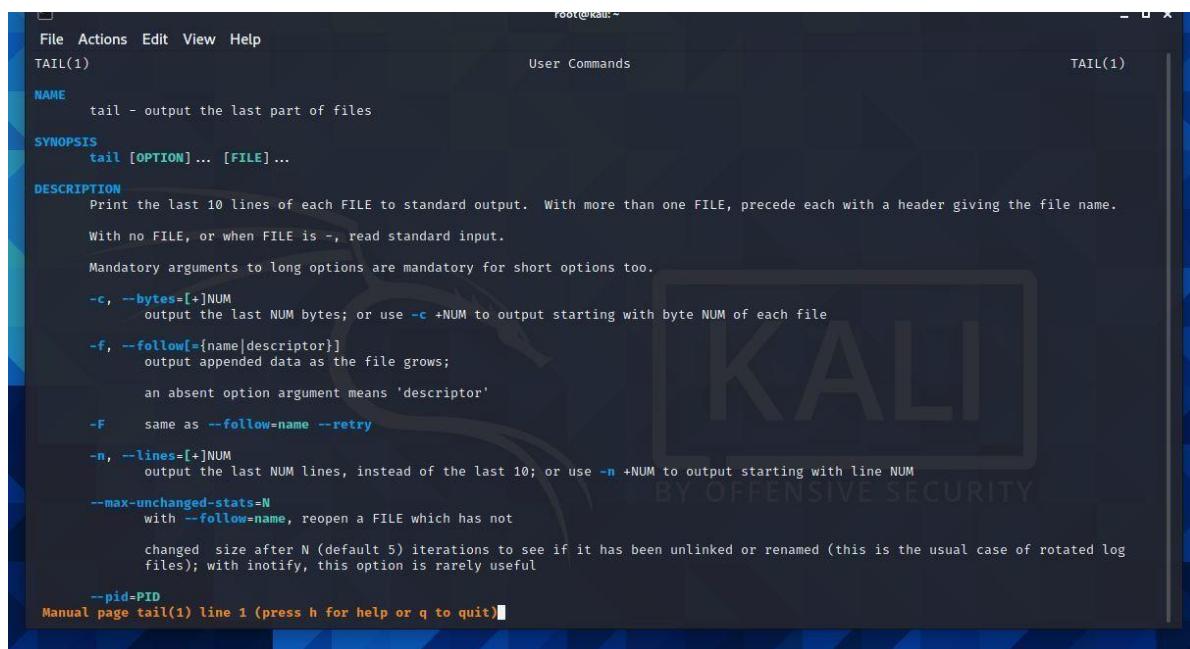
```
File Actions Edit View Help
zsh: corrupt history file /root/.zsh_history
[~]
# pwd
/root
[~]
# history
 1 ping google.com
 2 ip a
 3 nmap -sn 192.168.1.1/24
 4 pwd
 5 sysinfo
 6 systeminfo
 7 hostname
 8 vim test
 9 ls
10 vim test
11 ls
12 rm test
13 ls
14 cal
15 whoami
16 nmap
17 ifconfig
18 clear
19 netdiscover
20 pwd
[~]
#
```

The background of the terminal window features the Kali Linux logo and the text "BY OFFENSIVE SECURITY".

man

man command in Linux is used to display the user manual of any command that we can run on the terminal. It provides a detailed view of the command which includes NAME, SYNOPSIS, DESCRIPTION, OPTIONS, EXIT STATUS, RETURN VALUES, ERRORS, FILES, VERSIONS, EXAMPLES, AUTHORS and SEE ALSO.

```
—(root💀 kali)#[~]
# man tail
—(root💀 kali)#[~]
```



```
File Actions Edit View Help
TAIL(1)                               User Commands                               TAIL(1)
NAME          tail - output the last part of files
SYNOPSIS      tail [OPTION] ... [FILE] ...
DESCRIPTION   Print the last 10 lines of each FILE to standard output. With more than one FILE, precede each with a header giving the file name.
              With no FILE, or when FILE is -, read standard input.
              Mandatory arguments to long options are mandatory for short options too.
-c, --bytes=[+]NUM
              output the last NUM bytes; or use -c +NUM to output starting with byte NUM of each file
-f, --follow[={name|descriptor}]
              output appended data as the file grows;
              an absent option argument means 'descriptor'
-F           same as --follow=name --retry
-n, --lines=[+]NUM
              output the last NUM lines, instead of the last 10; or use -n +NUM to output starting with line NUM
--max-unchanged-stats=N
              with --follow=name, reopen a FILE which has not
              changed size after N (default 5) iterations to see if it has been unlinked or renamed (this is the usual case of rotated log
              files); with inotify, this option is rarely useful
--pid=PID
Manual page tail(1) line 1 (press h for help or q to quit)
```

cd

cd command in linux known as change directory command. It is used to change current working directory.

Syntax:

```
$ cd [directory]
```

To move inside a subdirectory : to move inside a subdirectory in linux we use

```
$ cd [directory_name]
```

```
--(root㉿kali)-[~]
# cd college
--(root㉿kali)-[/college]
# cd exam
--(root㉿kali)-[/college/exam]
# cd nano.save
d: not a directory: nano.save
--(root㉿kali)-[/college/exam]
# cd ...
--(root㉿kali)-[/college]
# cd -
/collage/exam
--(root㉿kali)-[/college/exam]
# |
```

ls

ls is a Linux shell command that lists directory contents of files and directories

ls -a, list all files including hidden file starting with ‘.’

ls -d, list directories — with ‘*/’.

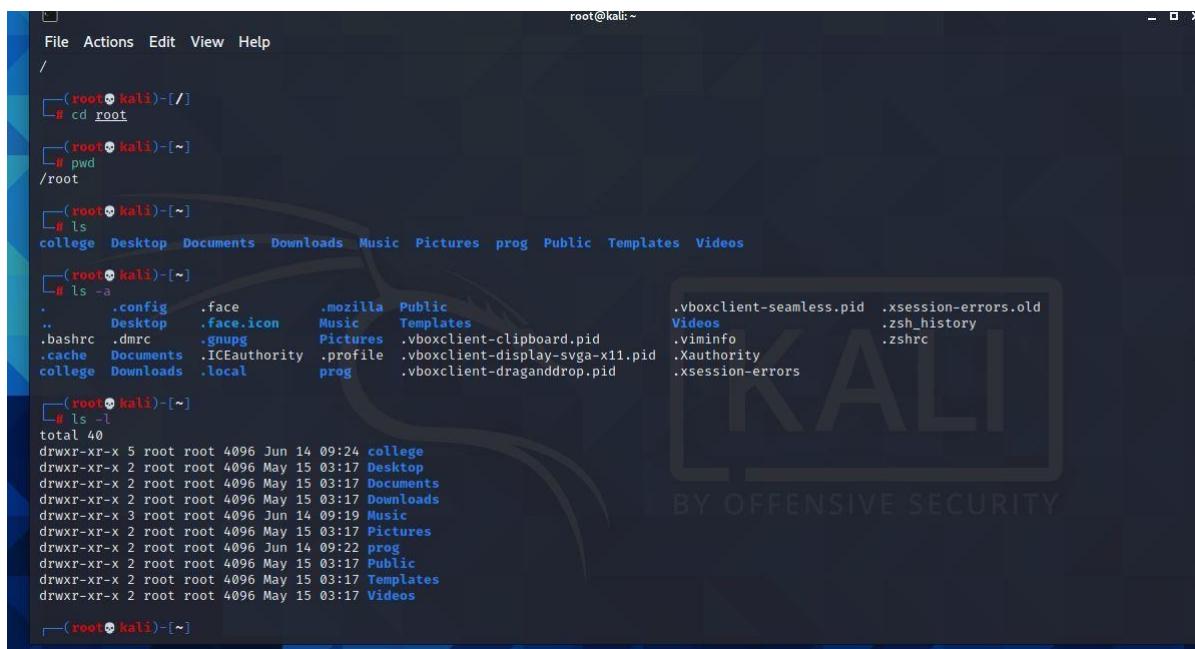
ls -i, list the index number of each file.

ls -l, list with long format — show permissions.

ls -s, list file size.

ls -la, list long format including hidden files.

ls -ls, list with long format with file size.



The screenshot shows a terminal window titled 'root@kali: ~'. The user has run several commands to demonstrate the ls command:

- cd root
- pwd
- ls
- ls -a
- ls -l
- ls -ls

The final output of the ls -ls command is as follows:

```
total 40
drwxr-xr-x 5 root root 4096 Jun 14 09:24 college
drwxr-xr-x 2 root root 4096 May 15 03:17 Desktop
drwxr-xr-x 2 root root 4096 May 15 03:17 Documents
drwxr-xr-x 2 root root 4096 May 15 03:17 Downloads
drwxr-xr-x 3 root root 4096 Jun 14 09:19 Music
drwxr-xr-x 2 root root 4096 May 15 03:17 Pictures
drwxr-xr-x 2 root root 4096 Jun 14 09:22 prog
drwxr-xr-x 2 root root 4096 May 15 03:17 Public
drwxr-xr-x 2 root root 4096 May 15 03:17 Templates
drwxr-xr-x 2 root root 4096 May 15 03:17 Videos
```

20MCA136 - Networking & System Administration Lab

```
File Actions Edit View Help
root@kali:[~]
# ls -R
.:
college Desktop Documents Downloads Music Pictures prog Public Templates Videos
./college:
exam lab work
./college/exam:
nano.save
./college/lab:
./college/work:
./Desktop:
./Documents:
./Downloads:
./Music:
college
./Music/college:
./Pictures:
./prog:
./Public:
./Templates:
./Videos:

root@kali:[~]
```

```
File Actions Edit View Help
root@kali:[~]
# ls --version
ls (GNU coreutils) 8.32
Copyright (C) 2020 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <https://gnu.org/licenses/gpl.html>.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Written by Richard M. Stallman and David MacKenzie.

root@kali:[~]
# ls ..
bin dev home initrd.img.old lib32 libx32 media opt root sbin sys usr vmlinuz
boot etc initrd.img lib lib64 lost+found mnt proc run srv tmp var vmlinuz.old

root@kali:[~]
# ls =
college Desktop Documents Downloads Music Pictures prog Public Templates Videos
root@kali:[~]
# ls -l
total 40
drwxr-xr-x 5 root root 4096 Jun 14 09:24 college
drwxr-xr-x 2 root root 4096 Jun 14 09:22 prog
drwxr-xr-x 3 root root 4096 Jun 14 09:19 Music
drwxr-xr-x 2 root root 4096 May 15 03:17 Desktop
drwxr-xr-x 2 root root 4096 May 15 03:17 Documents
drwxr-xr-x 2 root root 4096 May 15 03:17 Downloads
drwxr-xr-x 2 root root 4096 May 15 03:17 Pictures
drwxr-xr-x 2 root root 4096 May 15 03:17 Public
drwxr-xr-x 2 root root 4096 May 15 03:17 Templates
drwxr-xr-x 2 root root 4096 May 15 03:17 Videos

root@kali:[~]
# ls -r
Videos Templates Public prog Pictures Music Downloads Documents Desktop college
root@kali:[~]
```

mkdir

to as folders in some operating systems). This command can create multiple directories at once as well as set the permissions for the directories. It is mkdir command in Linux allows the user to create directories (also referred important to note that the user executing this command must have enough permissions to create a directory

in the parent directory, or he/she may receive a ‘permission denied’ error.

Syntax:

mkdir [options...] [directories ...]

- ② --version: It displays the version number, some information regarding the license and exits.

Syntax:

mkdir --version



A terminal window showing a root shell on Kali Linux. The user runs several ls commands to show the contents of their home directory (~) and then creates two new directories: 'college' and 'assignments'. Finally, they change into the 'college' directory and list its contents.

```
(root💀kali㉿kali:~)
# ls -r
Videos Templates Public prog Pictures Music Downloads Documents Desktop college
(root💀kali㉿kali:~)
# ls
college Desktop Documents Downloads Music Pictures prog Public Templates Videos
(root💀kali㉿kali:~)
# mkdir amal jyothi
(root💀kali㉿kali:~)
# ls
amal college Desktop Documents Downloads jyothi Music Pictures prog Public Templates Videos
(root💀kali㉿kali:~)
# cd college
(root💀kali㉿kali:[~/college])
# mkdir assignments
(root💀kali㉿kali:[~/college])
# ls
assignments exam lab work
(root💀kali㉿kali:[~/college])
#
```

touch

The touch command is a standard command used in UNIX/Linux operating system which is used to create, change and modify timestamps of a file. Basically, there are two different commands to create a file in the Linux system which is as follows:

- ② cat command: It is used to create the file with content.
- ② touch command: It is used to create a file without any content. The file created using touch command is empty. This command can be used when the user doesn't have data to store at the time of file creation.



```
(root💀 kali) [~/college]
└─# touch java
(root💀 kali) [~/college]
└─# ls
assignments  exam  java  lab  work
(root💀 kali) [~/college]
└─# cd exam
(root💀 kali) [~/college/exam]
└─# touch exam1
(root💀 kali) [~/college/exam]
└─# ls
exam1  nano.save
(root💀 kali) [~/college/exam]
```

rmdir

If you need to delete a directory, use the rmdir command. However, rmdir only allows you to delete empty directories.

rm

rm stands for remove here. rm command is used to remove objects such as files, directories, symbolic links and so on from the file system like UNIX. To be more precise, rm removes references to objects from the filesystem, where those objects might have had multiple references (for example, a file with two different names). By default, it does not remove directories.

This command normally works silently and you should be very careful while running rm command because once you delete the files then you are not able to recover the contents of files and directories.

Syntax:

```
rm [OPTION]... FILE...
```

Let us consider 5 files having name a.txt, b.txt and so on till e.txt.

```
$ ls
```

```
a.txt b.txt c.txt d.txt e.txt
```

Removing one file at a time

```
$ rm a.txt
```

```
$ ls
```

```
b.txt c.txt d.txt e.txt
```

Removing more than one file at a time

```
$ rm b.txt c.txt
```

```
$ ls
```

d.txt e.txt

```
File Actions Edit View Help
zsh: corrupt history file /root/.zsh_history
[root@kali ~]
# pwd
/root
[root@kali ~]
# rm -r prog
[root@kali ~]
# ls
animal college Desktop Documents Downloads java jyothi Music Pictures Public Templates Videos
[root@kali ~]
# rm -r jyothi
[root@kali ~]
# ls
animal college Desktop Documents Downloads Music Pictures Public Templates Videos
[root@kali ~]
# rm -f java
[root@kali ~]
# ls
animal college Desktop Documents Downloads Music Pictures Public Templates Videos
[root@kali ~]
#
```

cat

Cat(concatenate) command is very frequently used in Linux. It reads data from the file and gives their content as output. It helps us to create, view, concatenate files. So let us see some frequently used cat commands.

- 1) To view a single file

Command:

```
$cat filename
```

Output

It will show content of given filename

- 2) To view multiple files

Command:

```
$cat file1 file2
```



The screenshot shows a terminal window with a dark background and light-colored text. The text is a session of the 'cat' command being used to read files. The session starts with 'cat cls', followed by the contents of the file 'cls'. Then, 'cat java.txt' is run, followed by the contents of the file 'java.txt'. Finally, 'cat > java.txt' is run, which creates a new file 'java.txt' containing the previous output. The terminal prompt is '(root㉿kali)-[~/college/lab]'.

```
(root㉿kali)-[~/college/lab]
# cat cls
hi all
good mornig
how are you all

(root㉿kali)-[~/college/lab]
# cat java.txt

cat > java.txt
clear

(root㉿kali)-[~/college/lab]
# █
```

echo

echo command in linux is used to display line of text/string that are passed as an argument . This is a built in command that is mostly used in shell scripts and batch files to output status text to the screen or a file.

Syntax :

echo [option] [string]

```
__(root㉿kali)-[~/college]
# nano java

__(root㉿kali)-[~/college]
# echo hii all>> java

__(root㉿kali)-[~/college]
# ls
assignments exam java lab work

__(root㉿kali)-[~/college]
# nano java
ngjgjhjgk
hii all

__(root㉿kali)-[~/college]
# echo nimisha james mca -b >>nm.txt

__(root㉿kali)-[~/college]
# ls
assignments exam java lab nm.txt work

__(root㉿kali)-[~/college]
# cat nm.txt
nimisha james mca -b

__(root㉿kali)-[~/college]
#
```

head

It is the complementary of Tail command. The head command, as the name implies, print the top N number of data of the given input. By default, it prints the first 10 lines of the specified files. If more than one file name is provided then data from each file is preceded by its file name.

Syntax:

```
head [OPTION]... [FILE]...
```

Let us consider two files having name state.txt and capital.txt contains all the names of the Indian states and capitals respectively.

```
[root@kali ~]# head nm.txt
[root@kali ~]# head nm.txt
hi all
how are you
monday
sunday

[root@kali ~]# nano nm.txt
[root@kali ~]# head nm.txt
hey
hleo
001
amal jythoi
philos
mysore
bngkr
php lab
python
js

[root@kali ~]# head -n 5 nm.txt
hey
hleo
001
amal jythoi
philos

[root@kali ~]#
```

tail

It is the complementary of head command. The tail command, as the name implies, print the last N number of data of the given input. By default it prints the last 10 lines of the specified files. If more than one file name is provided then data from each file is preceded by its file name.

The screenshot shows a terminal window on a Kali Linux system. The terminal window has a dark background with a stylized dragon logo in the center. The window title is "Terminal". The menu bar includes "File", "Actions", "Edit", "View", and "Help". The terminal session shows the following commands and output:

```
File Actions Edit View Help
hleo
001
amal jythoi
philos
mysore
bngkr
php lab
python
js

[~(root💀 kali)-[~/college]
└# nano nm.txt

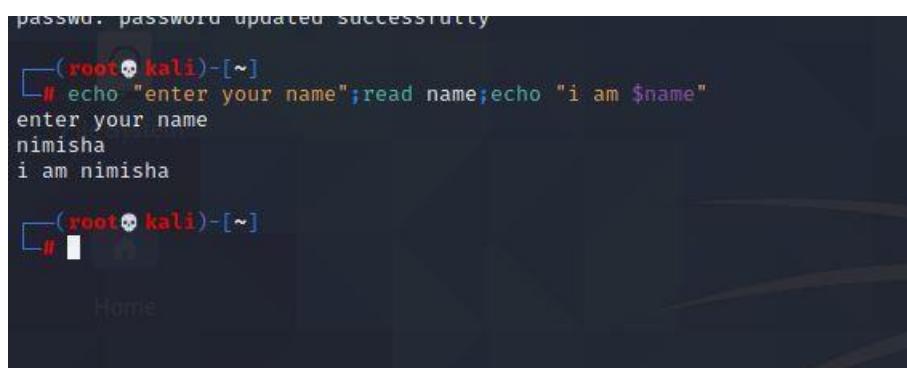
[~(root💀 kali)-[~/college]
└# tail nm.txt
bngkr
php lab
python
js
java
hi all
how are you
monday
sunday

[~(root💀 kali)-[~/college]
└# tail -n 5 nm.txt
hi all
how are you
monday
sunday

[~(root💀 kali)-[~/college]
└# ]
```

read

read command in Linux system is used to read from a file descriptor. Basically, this command read up the total number of bytes from the specified file descriptor into the buffer. If the number or count is zero then this command may detect the errors. But on success, it returns the number of bytes read.

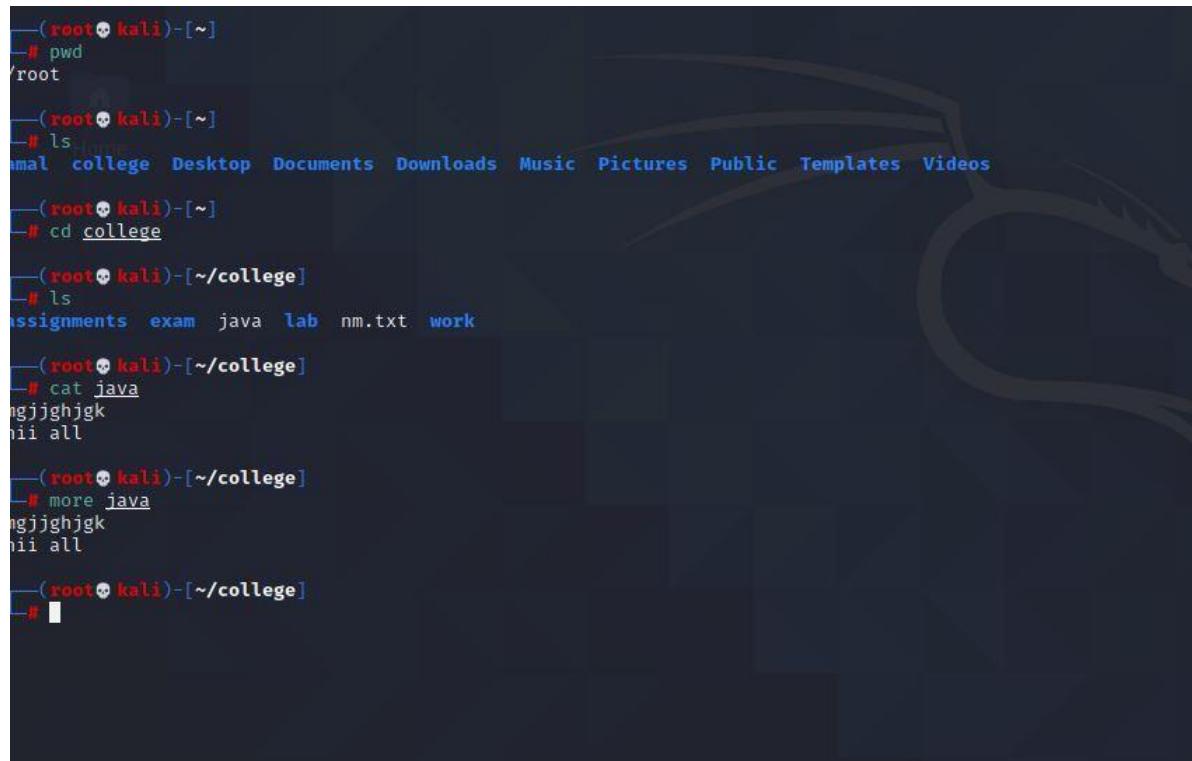


The screenshot shows a terminal window on a Kali Linux system. The terminal prompt is '(root💀 kali)'. The user runs the command '# echo "enter your name";read name;echo "i am \$name"' and enters 'nimisha' when prompted. The output shows 'i am nimisha'.

```
password updated successfully
(root💀 kali)-
# echo "enter your name";read name;echo "i am $name"
enter your name
nimisha
i am nimisha
(root💀 kali)-
#
```

more

more command is used to view the text files in the command prompt, displaying one screen at a time in case the file is large (For example log files). The more command also allows the user do scroll up and down through the page. The syntax along with options and command is as follows. Another application of more is to use it with some other command after a pipe. When the output is large, we can use more command to see output one by one.



```
__(root㉿kali)-[~]
└─# pwd
/root

__(root㉿kali)-[~]
└─# ls
mal college Desktop Documents Downloads Music Pictures Public Templates Videos

__(root㉿kali)-[~]
└─# cd college
ssignments exam java lab nm.txt work

__(root㉿kali)-[~/college]
└─# ls
gjighjgk
iii all

__(root㉿kali)-[~/college]
└─# cat java
gjighjgk
iii all

__(root㉿kali)-[~/college]
└─# more java
gjighjgk
iii all

__(root㉿kali)-[~/college]
└─#
```

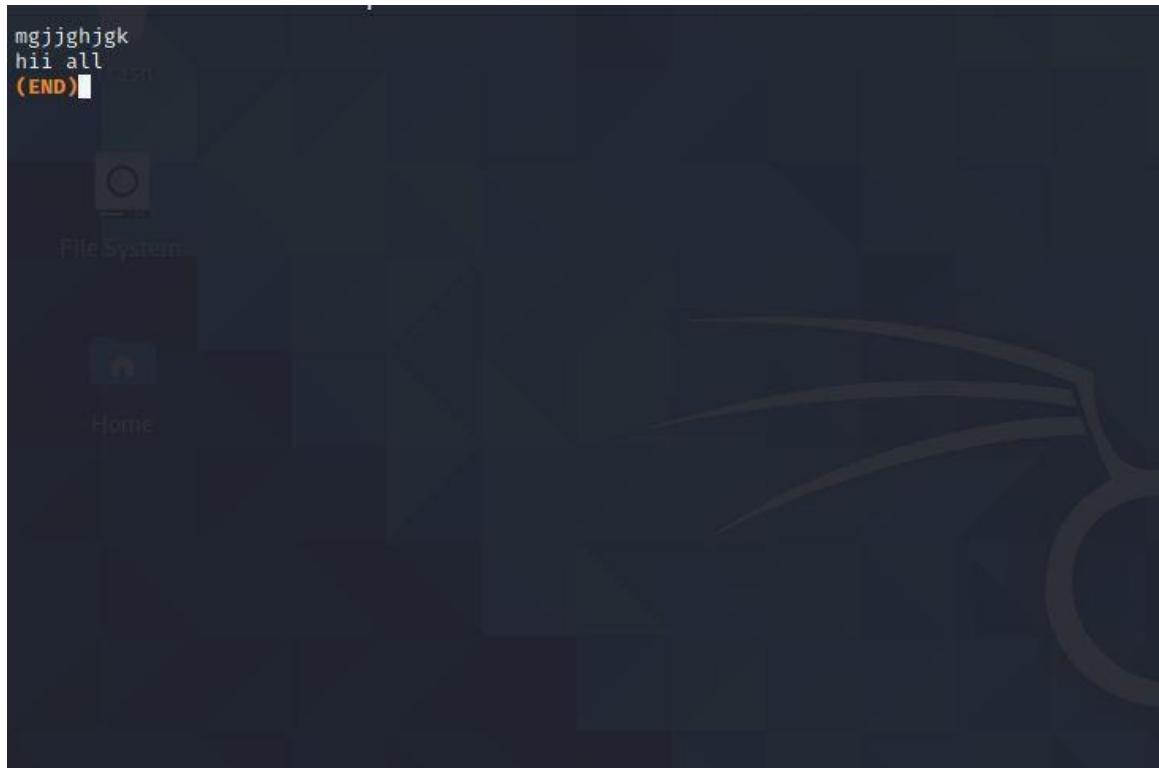
less

Less command is linux utility which can be used to read contents of text file one page(one screen) per time. It has faster access because if file is large, it don't access complete file, but access it page by page.

For example, if it's a large file and you are reading it using any text editor, then the complete file will be loaded to main memory, but less command don't load entire file, but load it part by part, which makes it faster.

syntax :

less filename



cut

The cut n 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 option with command otherwise it gives error. If more than one file name is provided then data from each file is not preceded by its file name.

Syntax:

cut OPTION... [FILE]...

```
(root@kali)-[~/college/exam]
# pwd
/root/college/exam

[root@kali]-[~/college/exam]
# cd ..
[root@kali]-[~/college]
# cd ..
[root@kali]-[~]
# ls
amal college Desktop Documents Downloads Music Pictures Public Templates Videos

[root@kali]-[~]
# cd college
[root@kali]-[~/college]
# ls
assignments exam lab nm.txt work

[root@kali]-[~/college]
# cut nm.txt
cut: you must specify a list of bytes, characters, or fields
Try 'cut --help' for more information.

[root@kali]-[~/college]
# paste nm.txt
mgi jghjgk
hi all

[root@kali]-[~/college]
```

paste

Paste command is one of the useful commands in Unix or Linux operating system. It is used to join files horizontally (parallel merging) by outputting lines consisting of lines from each file specified, separated by tab as delimiter, to the standard output. When no file is specified, or put dash (“-“) instead of file name, paste reads from standard input and gives output as it is until a interrupt command [Ctrl-c] is given. Syntax:

paste [OPTION]... [FILE]...

```
(root@kali)-[~/college/exam]
# pwd
/root/college/exam

(root@kali)-[~/college/exam]
# cd ..
[root@kali]-[~/college]
# cd ..

(root@kali)-[~]
# ls
amal college Desktop Documents Downloads Music Pictures Public Templates Videos

(root@kali)-[~]
# cd college
[root@kali]-[~/college]
# ls
assignments exam lab nm.txt work

(root@kali)-[~/college]
# cut nm.txt
cut: you must specify a list of bytes, characters, or fields
Try 'cut --help' for more information.

(root@kali)-[~/college]
# paste nm.txt
mgjighjgk
hi all

[root@kali]-[~/college]
```

uname

The command ‘uname’ displays the information about the system.

Syntax:

uname [OPTION]

1. -a option: It prints all the system information in the following order:
Kernel name, network node hostname, kernel release date, kernel version, machine hardware name, hardware platform, operating system

```
└─(root💀kali㉿kali)-[~]
  └─# uname -a
Linux kali 5.10.0-kali3-amd64 #1 SMP Debian 5.10.13-1kali1 (2021-02-08) x86_64 GNU/Linux

└─(root💀kali㉿kali)-[~]
  └─# uname -s
Linux

└─(root💀kali㉿kali)-[~]
  └─# uname -n
kali

└─(root💀kali㉿kali)-[~]
  └─# uname -v
#1 SMP Debian 5.10.13-1kali1 (2021-02-08)

└─(root💀kali㉿kali)-[~]
  └─#
```

cp

cp stands for copy. This command is used to copy files or group of files or directory. It creates an exact image of a file on a disk with different file name. cp command require at least two filenames in its arguments.

Syntax:

```
cp [OPTION] Source Destination  
cp [OPTION] Source Directory  
cp [OPTION] Source-1 Source-2 Source-3 Source-n Directory
```

First and second syntax is used to copy Source file to Destination file or Directory. Third syntax is used to copy multiple Sources(files) to Directory.

```
[root@kali ~]# ls  
amal college Desktop Documents Downloads Music Pictures Public Templates Videos  
[root@kali ~]# cd college  
[root@kali ~/college]# ls  
assignments exam java lab nm.txt work  
[root@kali ~/college]# cp java nm.txt  
[root@kali ~/college]# cat nm.txt  
mgjighjgk  
hii all  
[root@kali ~/college]#
```

mv

mv stands for move. mv is used to move one or more files or directories from one place to another in a file system like UNIX. It has two distinct functions:

- (i) It renames a file or folder.
- (ii) It moves a group of files to a different directory.

No additional space is consumed on a disk during renaming. This command normally works silently means no prompt for confirmation.

Syntax:

mv [Option] source destination

```
[root@kali ~]
# uname -v
#1 SMP Debian 5.10.13-1kali1 (2021-02-08)

[root@kali ~]
# ls
amal college Desktop Documents Downloads Music Pictures Public Templates Videos

[root@kali ~]
# cd college
[root@kali ~college]
# ls
assignments exam java lab nm.txt work

[root@kali ~college]
# cp java nm.txt
[root@kali ~college]
# cat nm.txt
mgjghjgk
hii all

[root@kali ~college]
# mv java nm.txt
[root@kali ~college]
# cat nm.txt
mgjghjgk
hii all

[root@kali ~college]
# locate ■
```

locate

locate command in Linux is used to find the files by name. There are two most widely used file searching utilities accessible to users called find and locate. The locate utility works better and faster than find command counterpart because instead of searching the file system when a file search is initiated, it would look through a database. This database contains bits and parts of files and their corresponding paths on your system. By default, locate command does not check whether the files found in the database still exist and it never reports files created after the most recent update of the relevant database.

Syntax:

locate [OPTION]... PATTERN...

find

The find command in UNIX is a command line utility for walking a file hierarchy. It can be used to find files and directories and perform subsequent operations on them. It supports searching by file, folder, name, creation date, modification date, owner and permissions. By using the ‘-exec’ other UNIX commands can be executed on files or folders found.

Syntax :

```
$ find [where to start searching from]  
[expression determines what to find] [-options] [what to find]
```

grep

The grep filter searches a file for a particular pattern of characters, and displays all lines that contain that pattern. The pattern that is searched in the file is referred to as the regular expression (grep stands for globally search for regular expression and print out).

Syntax:

```
grep [options] pattern [files]
```

```
(root㉿kali)-[~/college]
└─# paste nm.txt
mgjgjhgjgk
hi all

(roots㉿kali)-[~/college]
└─# find .
./assignments
./nm.txt
./lab
./lab/java.txt
./lab/cls
./exam
./exam/nano.save
./exam/hhh.txt
./work

(roots㉿kali)-[~/college]
└─# pwd
/root/college

(roots㉿kali)-[~/college]
└─# ls
assignments exam lab nm.txt work

(roots㉿kali)-[~/college]
└─# locate ".txt"
Usage: grep [OPTION] ... PATTERNS [FILE] ...
Try 'grep --help' for more information.

(roots㉿kali)-[~/college]
└─# df
Filesystem      1K-blocks    Used Available Use% Mounted on
udev            1501308      0   1501308   0% /dev
tmpfs           307240   1004   306236   1% /run
/dev/sda1       81000912 9280388  67559912  13% /
tmpfs           1536180      0   1536180   0% /dev/shm
tmpfs             5120      0    5120   0% /run/lock
tmpfs           307236      56   307180   1% /run/user/0
tmpfs           307236     48   307188   1% /run/user/1000

(roots㉿kali)-[~/college]
└─# du
4      ./assignments
12     ./lab
4      ./exam/hhh.txt
```

df

The df command (short for disk free), is used to display information related to file systems about total space and available space.

Syntax :

df [OPTION]... [FILE]...



```
File Actions Edit View Help
└─(root㉿kali)-[~]
# df
Filesystem      1K-blocks    Used Available Use% Mounted on
udev             1501308      0   1501308  0% /dev
tmpfs            307240     932   306308  1% /run
/dev/sda1        81000912 9223164  67617136 13% /
tmpfs            1536180      0   1536180  0% /dev/shm
tmpfs             5120       0    5120  0% /run/lock
tmpfs            307236      56   307180  1% /run/user/0
└─(root㉿kali)-[~]
# du
4      ./Documents
4      ./local/share/icc
4      ./local/share/nano
12     ./local/share
16     ./local
8      ./config/qterminal.org
12     ./config/Thunar
4      ./config/xfce4/xfwm4
8      ./config/xfce4/desktop
8      ./config/xfce4/panel/launcher-6
8      ./config/xfce4/panel/launcher-7
24     ./config/xfce4/panel
68     ./config/xfce4/xfconf
72     ./config/xfce4/xfconf
112    ./config/xfce4
8      ./config/dconf
8      ./config/gtk-3.0
8      ./config/qt5ct
84     ./config/pulse
252    ./config
4      ./Desktop
4      ./mozilla/extensions
4      ./mozilla/firefox/Pending Pings
```

du

- du command, short for disk usage, is used to estimate file space usage.
- The du command can be used to track the files and directories which are consuming excessive amount of space on hard disk drive. Syntax :
- du [OPTION]... [FILE]...
- du [OPTION]... --files=from=F

```
(root💀kali)-[~]
# du
4      ./Documents
4      ./local/share/icc
4      ./local/share/nano
12     ./local/share
16     ./local
8      ./config/qterminal.org
12     ./config/Thunar
4      ./config/xfce4/xfwm4
8      ./config/xfce4/desktop
8      ./config/xfce4/panel/launcher-6
8      ./config/xfce4/panel/launcher-7
24     ./config/xfce4/panel
68     ./config/xfce4/xfconf/xfc-perchannel-xml
72     ./config/xfce4/xfconf
112    ./config/xfce4
8      ./config/dconf
8      ./config/gtk-3.0
8      ./config/qt5ct
84     ./config/pulse
252    ./config
4      ./Desktop
4      ./mozilla/extensions
4      ./mozilla/firefox/Pending Pings
8      ./mozilla/firefox/avgxuq93.default
4      ./mozilla/firefox/Crash Reports/events
12     ./mozilla/firefox/Crash Reports
744    ./mozilla/firefox/0et6gbu1.default-esr/security_state
4      ./mozilla/firefox/0et6gbu1.default-esr/crashes/events
12     ./mozilla/firefox/0et6gbu1.default-esr/crashes
4      ./mozilla/firefox/0et6gbu1.default-esr/extensions
4      ./mozilla/firefox/0et6gbu1.default-esr/bookmarkbackups
12     ./mozilla/firefox/0et6gbu1.default-esr/datarereporting
60     ./mozilla/firefox/0et6gbu1.default-esr/sessionstore-backups
```

useradd

useradd is a command in Linux that is used to add user accounts to your system. It is just a symbolic link to adduser command in Linux and the difference between both of them is that useradd is a native binary compiled with system whereas adduser is a Perl script which uses useradd binary in the background. It make changes to the following files:

- /etc/passwd
- /etc/shadow
- /etc/group
- /etc/gshadow
- creates a directory for new user in /home

```
(root㉿kali)-[~]
# userdel
Usage: userdel [options] LOGIN

Options:
  -f, --force           force removal of files,
                        even if not owned by user
  -h, --help            display this help message and exit
  -r, --remove          remove home directory and mail spool
  -R, --root CHROOT_DIR
  -P, --prefix PREFIX_DIR
  -Z, --selinux-user   remove any SELinux user mapping for the user

(root㉿kali)-[~]
# useradd
Usage: useradd [options] LOGIN
      useradd -D
      useradd -D [options]

Options:
  --badnames            do not check for bad names
  -b, --base-dir BASE_DIR        base directory for the home directory of the
                                    new account
  --btrfs-subvolume-home       use BTRFS subvolume for home directory
  -c, --comment COMMENT      GECOS field of the new account
  -d, --home-dir HOME_DIR     home directory of the new account
  -D, --defaults            print or change default useradd configuration
  -e, --expiredate EXPIRE_DATE expiration date of the new account
  -f, --inactive INACTIVE    password inactivity period of the new account
  -g, --gid GROUP           name or ID of the primary group of the new
                            account
  -G, --groups GROUPS       list of supplementary groups of the new
                            account
  -h, --help                display this help message and exit
  -k, --skel SKEL_DIR        use this alternative skeleton directory
  -K, --key KEY=VALUE        override /etc/login.defs defaults
  -l, --no-log-init         do not add the user to the lastlog and
                            faillog databases
```

userdel

userdel command in Linux system is used to delete a user account and related files. This command basically modifies the system account files, deleting all the entries which refer to the username LOGIN. It is a low-level utility for removing the users.

Syntax:

`userdel [options] LOGIN`

```
(root💀 kali)㉿ ~
# userdel
Usage: userdel [options] LOGIN

Options:
  -f, --force           force removal of files,
                        even if not owned by user
  -h, --help            display this help message and exit
  -r, --remove          remove home directory and mail spool
  -R, --root CHROOT_DIR
  -P, --prefix PREFIX_DIR
  -Z, --selinux-user   remove any SELinux user mapping for the user

--(root💀 kali)㉿ ~
# useradd
Usage: useradd [options] LOGIN
      useradd -D
      useradd -D [options]

Options:
  --badnames           do not check for bad names
  -b, --base-dir BASE_DIR
                      base directory for the home directory of the
                      new account
  --btrfs-subvolume-home
  -c, --comment COMMENT
  -d, --home-dir HOME_DIR
  -D, --defaults
  -e, --expiredate EXPIRE_DATE
  -f, --inactive INACTIVE
  -g, --gid GROUP
  -G, --groups GROUPS
  -h, --help            display this help message and exit
  -k, --skel SKEL_DIR
  -K, --key KEY-VALUE
  -l, --no-log-init    do not add the user to the lastlog and
                      faillog databases
```

sudo

The sudo command allows you to run programs as another user, by default the root user. If you spend a lot of time on the command line, sudo is one of the commands that you will use quite frequently.

Using sudo instead of login in as root is more secure because you can grant limited administrative privileges to individual users without them knowing the root password.

```
(root💀kali)-[~]
└─# sudo
usage: sudo -h | -K | -k | -V
usage: sudo -v [-AknS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-AknS] [-g group] [-h host] [-p prompt] [-U user] [-u user] [command]
usage: sudo [-AbEHknPS] [-r role] [-t type] [-C num] [-D directory] [-g group] [-h host] [-p prompt] [-R directo
    [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-AknS] [-r role] [-t type] [-C num] [-D directory] [-g group] [-h host] [-p prompt] [-R directo
...
[root💀kali)-[~]
└─# sudo useradd nabin

(root💀kali)-[~]
└─# sudo -h
sudo - execute a command as another user

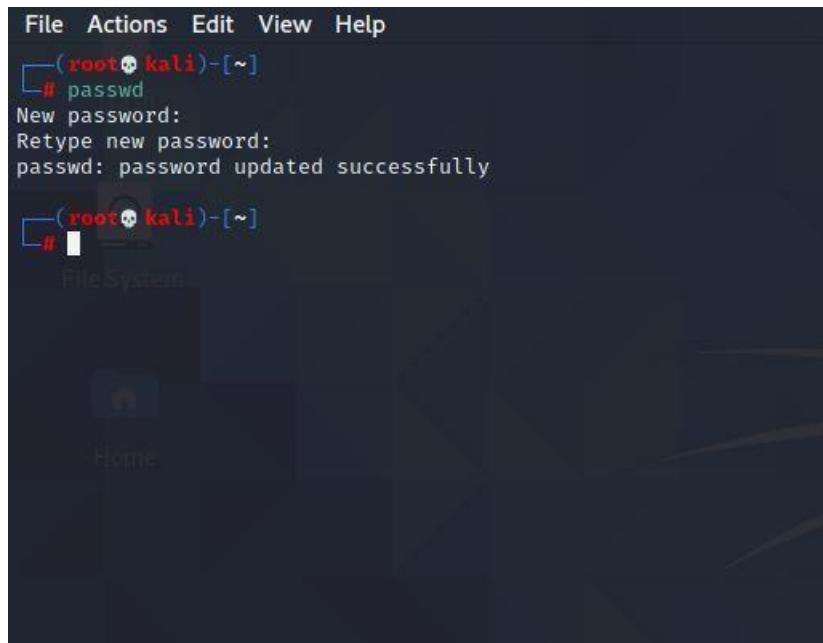
usage: sudo -h | -K | -k | -V
usage: sudo -v [-AknS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-AknS] [-g group] [-h host] [-p prompt] [-U user] [-u user] [command]
usage: sudo [-AbEHknPS] [-r role] [-t type] [-C num] [-D directory] [-g group] [-h host] [-p prompt] [-R directo
    [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-AknS] [-r role] [-t type] [-C num] [-D directory] [-g group] [-h host] [-p prompt] [-R directo
...
Options:
  -A, --askpass           use a helper program for password prompting
  -b, --background        run command in the background
  -B, --bell              ring bell when prompting
  -C, --close-from=num   close all file descriptors ≥ num
  -D, --chdir=directory   change the working directory before running command
  -E, --preserve-env     preserve user environment when running command
  --preserve-env=list    preserve specific environment variables
  -e, --edit              edit files instead of running a command
  -g, --group=group       run command as the specified group name or ID
```

passwd

passwd command in Linux is used to change the user account passwords. The root user reserves the privilege to change the password for any user on the system, while a normal user can only change the account password for his or her own account.

Syntax:

```
passwd [options] [username]
```



The screenshot shows a terminal window with a dark background and light-colored text. At the top, there is a menu bar with options: File, Actions, Edit, View, Help. Below the menu, the terminal prompt shows the user is root on a Kali Linux system: `(root💀 kali)-[~]`. The user then runs the `passwd` command. The terminal asks for a new password, then re-prompts for confirmation. Finally, it displays the message `passwd: password updated successfully`. The terminal window is titled "Terminal" and has a "File System" tab visible at the bottom.

```
File Actions Edit View Help
└─(root💀 kali)-[~]
└─# passwd
New password:
Retype new password:
passwd: password updated successfully
└─(root💀 kali)-[~]
└─#
```

usermod

usermod command or modify user is a command in Linux that is used to change the properties of a user in Linux through the command line. After creating a user we have to sometimes change their attributes like password or login directory etc. so in order to do that we use the Usermod command. The information of a user is stored in the following files:

- /etc/passwd
- /etc/group
- /etc/shadow
- /etc/login.defs
- /etc/gshadow
- /etc/login.defs

When we execute usermod command in terminal the command makes the changes in these files itself.

```
(root㉿kali)-[~]
# usermod
Usage: usermod [options] LOGIN

Options:
  -b, --badnames      allow bad names
  -c, --comment COMMENT    new value of the GECOS field
  -d, --home HOME_DIR    new home directory for the user account
  -e, --expiredate EXPIRE_DATE  set account expiration date to EXPIRE_DATE
  -f, --inactive INACTIVE  set password inactive after expiration
                           to INACTIVE
  -g, --gid GROUP        force use GROUP as new primary group
  -G, --groups GROUPS   new list of supplementary GROUPS
  -a, --append           append the user to the supplemental GROUPS
                           mentioned by the -G option without removing
                           the user from other groups
  -h, --help             display this help message and exit
  -l, --login NEW_LOGIN  new value of the login name
  -L, --lock              lock the user account
  -m, --move-home        move contents of the home directory to the
                           new location (use only with -d)
  -o, --non-unique       allow using duplicate (non-unique) UID
  -p, --password PASSWORD  use encrypted password for the new password
  -R, --root CHROOT_DIR   directory to chroot into
  -P, --prefix PREFIX_DIR prefix directory where are located the /etc/* files
  -s, --shell SHELL       new login shell for the user account
  -u, --uid UID           new UID for the user account
  -U, --unlock            unlock the user account
  -v, --add-subuids FIRST-LAST  add range of subordinate uids
  -V, --del-subuids FIRST-LAST  remove range of subordinate uids
  -w, --add-subgids FIRST-LAST  add range of subordinate gids
  -W, --del-subgids FIRST-LAST  remove range of subordinate gids
  -Z, --selinux-user SEUSER  new SELinux user mapping for the user account
```

1. To add a comment for a user

```
usermod -c "This is test user"
```

```
test_user
```

```
(root💀 kali)-[~]
# usermod -c "This is test user" test_user

(root💀 kali)-[~]
# cat /etc/passwd | grep test_user
test_user:x:1002:1002:This is test user:/home/test_user:/bin/sh
```

2. To change the expiry date of a

```
usermod -e 2020-05-29 test_use
```

```
(root💀 kali)-[~]
# usermod -e 2021-01-21 test_user

(root💀 kali)-[~]
# chage -l test_user
Last password change : Aug 13, 2021
Password expires       : never
Password inactive      : never
Account expires        : Jan 21, 2021
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires : 7
```

3. To lock a user

```
sudo usermod -L test_user
```

4. To unlock a user

```
sudo usermod -U test_user
```

```
(root💀 kali)-[~]
# usermod -L test_user

(root💀 kali)-[~]
# usermod -u test_user
usermod: invalid user ID 'test_user'

(root💀 kali)-[~]
# usermod -U test_user

(root💀 kali)-[~]
#
```

5. To set an unencrypted password for the user

```
(root💀 kali)-[~]
# usermod -p test_password test_user

(root💀 kali)-[~]
# cat /etc/shadow | grep test_user
test_user:test_password:18852:0:99999:7::18648:

(root💀 kali)-[~]
#
```

Groupadd

The groupadd command creates a new group account using the values specified on the commandline and the default values from the system. The new group will be entered into the system files as needed.

```
(root㉿kali)-[~]
└─# groupadd
Usage: groupadd [options] GROUP

Options:
  -f, --force          exit successfully if the group already exists,
                       and cancel -g if the GID is already used
  -g, --gid GID        use GID for the new group
  -h, --help           display this help message and exit
  -K, --key KEY=VALUE  override /etc/login.defs defaults
  -o, --non-unique     allow to create groups with duplicate
                       (non-unique) GID
  -p, --password PASSWORD  use this encrypted password for the new group
  -r, --system          create a system account
  -R, --root CHROOT_DIR  directory to chroot into
  -P, --prefix PREFIX_DIR  directory prefix
```

1. To add a new

groupadd groupname

groupname

```
(root㉿kali)-[~]
└─# addgroup groupname
Adding group `groupname' (GID 1003) ...
Done.

(root㉿kali)-[~]
└─#
```

2. To display version

addgroup --

version

```
(root㉿kali)-[~]
└─# addgroup --version
adduser version 3.118

Adds a user or group to the system.

Copyright (C) 1997, 1998, 1999 Guy Maor <maor@debian.org>
Copyright (C) 1995 Ian Murdock <imurdock@gnu.ai.mit.edu>,
               Ted Hajek <tedhajek@boombox.micro.umn.edu>

This program is free software; you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation; either version 2 of the License, or (at
your option) any later version.

This program is distributed in the hope that it will be useful, but
WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
General Public License, /usr/share/common-licenses/GPL, for more details.

(root㉿kali)-[~]
└─#
```

Groups

In linux, there can be multiple users(those who use/operate the system), and groups are nothing but the collection of users. Groups make it easy to manage users with the same security and access privileges. A user can be part of different groups.

Important Points:

- Groups command prints the names of the primary and any supplementary groups for each given username, or the current process if no names are given.
- If more than one name is given, the name of each user is printed before the list of that user's groups and the username is separated from the group list by a colon.

Syntax:

`groups [username]...`

```
—(root💀kali㉿kali:~)
# groupadd usrgrp

—(root💀kali㉿kali:~)
# groups
root:kaboxer
```

groupmod

groupmod command in Linux is used to modify or change the existing group on Linux system. It can be handled by superuser or root user. Basically, it modifies a group definition on the system by modifying the right entry in the database of the group.

Syntax:

`groupmod [option] GROUP`

```
—(root💀kali㉿kali:~)
# 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
  -o, --non-unique         change the name to NEW_GROUP
  -p, --password PASSWORD
                           allow to use a duplicate (non-unique) GID
                           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/* files

—(root💀kali㉿kali:~)
#
```

```
(root@kali㉿kali)-[~]
# groupadd mygrp

(root@kali㉿kali)-[~]
# groupmod -n bettergroup mygrp

(root@kali㉿kali)-[~]
# 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
  -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/* files

(root@kali㉿kali)-[~]
# groupmod -g 3000 bettergroup

(root@kali㉿kali)-[~]
# groupmod -g 777 3000
groupmod: group '3000' does not exist
```

groupdel

groupdel command is used to delete a existing group. It will delete all entry that refers to the group, modifies the system account files, and it is handled by superuser or root user.

Syntax:
groupdel [options] GROUP

```
(root@kali㉿kali)-[~]
# groupdel
Usage: groupdel [options] GROUP

Options:
  -h, --help              display this help message and exit
  -R, --root CHROOT_DIR  directory to chroot into
  -P, --prefix PREFIX_DIR prefix directory where are located the /etc/* files
  -f, --force              delete group even if it is the primary group of a user

(root@kali㉿kali)-[~]
# groupdel bettergroup

(root@kali㉿kali)-[~]
# groupdel -h
Usage: groupdel [options] GROUP
```

Chmod

In Unix-like operating systems, the *chmod* command is used to change the access mode of a file.

The name is an abbreviation of change mode. Syntax :

chmod [reference][operator][mode] file...

Options:

The *chmod* command supports the following command-line options:

-c, --changes: It is similar to the verbose option, but the difference is that it is reported if a change has been made.

-f, --silent, --quiet: It is used to suppress the error messages.

-v, --verbose: It is used to display a diagnostic for every processed file.

--no-preserve-root: It is used for not treating the backslash symbol ('/'), especially (the default)

--preserve-root: If this option is used, it will fail to operate recursively on backslash ('/').

--reference=RFILE: It is used to specify the RFILE's mode alternatively MODE values.

-R, --recursive: It is used to change files and directories recursively.

--help: It is used to display the help manual having a brief description of usage and supportoptions.

--version: It is used to display the version information.

```
root@kali:~# chmod g+rw myfile2.txt
```

```
-rw-r--r-- 1 root root 10 Aug 12 13:01 myfile2.txt
```

```
-rw-rw-r-- 1 root root 10 Aug 12 13:01 myfile2.txt
```

chown

Linux chown command is used to change a file's ownership, directory, or symbolic link for a user or group. The chown stands for change owner. In Linux, each file is associated with a corresponding owner or group.

The Linux system may have multiple users. Every user has a unique name and user ID. If only a user is available in the system, the user will be the owner of each file.

The Linux system may have multiple users. Every user has a unique name and user ID. If only a user is available in the system, the user will be the owner of each file.

Users can be listed in different groups. The group allows us to set permission on the group level instead of setting permission on an individual level.

Options:

Following are the command-line options of the chown command:

-c, --changes: It is used to display the detailed output like verbose, but it is reported when only a change is made.

-f, --silent, --quiet: It is used to suppress the error messages.

-v, --verbose: It is used to display a diagnostic for every processed file.

--dereference: It is used to affect the referent of each symbolic link.

-h, --no-dereference: It is used to affect the symbolic links instead of any referenced file.

--from=CURRENT_OWNER:CURRENT_GROUP: It is used to change the specific owner and group.

--no-preserve-root: It is used for not treating the backslash ('/') especially.

--preserve-root: If the chown is failed to operate recursively on backslash ('/').

--reference=RFILE: It is used to specify the RFILE's owner and group rather than their values.

```
[root@kali:~/college]
# chmod g+rw nm.txt
[root@kali:~/college]
#
[root@kali:~/college]
# ls -l
total 20
drwxr-xr-x 2 root root 4096 Jun 14 11:55 assignments
drwxr-xr-x 3 root root 4096 Jun 21 12:23 exam
drwxr-xr-x 2 root root 4096 Jun 14 12:22 lab
-rw-rw-r-- 1 root root 18 Jun 20 10:36 nm.txt
drwxr-xr-x 2 root root 4096 Jun 14 09:24 work

[root@kali:~/college]
# ls -l nm.txt
-rw-rw-r-- 1 root root 18 Jun 20 10:36 nm.txt

[root@kali:~/college]
# chown master nm.txt
chown: invalid user: 'master'

[root@kali:~/college]
# chown test_user nm.txt

[root@kali:~/college]
# chown -c test_user nm.txt
```

id

id command in Linux is **used to find out user and group names** and numeric ID's (UID or group ID) of the current user or any other user in the server. List out all the groups a user belongs to. Display security context of the current user

```
[root@kali:~/college]
# id
uid=0(root) gid=0(root) groups=0(root),142(kaboxer)

[root@kali:~/college]
#
```

ps

The ps command is used to view currently running processes on the system. It helps us to determine which process is doing what in our system, how much memory it is using, how much CPU space it occupies, user ID, command name, etc .

The ps command may display different results for different systems because it displays information about the currently running process of a system.

Option	Function
<u>ps -ef/</u> <u>ps -aux</u>	List currently running process in full format
<u>ps -ax</u>	List currently running process

<u>ps -u <username></u>	List process for specific user
<u>ps -C <command></u>	List process for given command
<u>ps -p <PID></u>	List process with given PID
<u>ps -ppid <PPID></u>	List process with given ppid
<u>pstree</u>	Show process in hierarchy
<u>ps -L</u>	List all threads for a particular process
<u>ps --sort pmem</u>	Find memory leak
<u>ps -eo</u>	Show security information
<u>ps -U root -u root u</u>	Show process running by root

```

└─(root㉿kali)-[~/college]
# ps
  PID TTY      TIME CMD
2592 pts/0    00:00:06 zsh
3570 pts/0    00:00:00 ps

└─(root㉿kali)-[~/college]
# ps -a
  PID TTY      TIME CMD
3575 pts/0    00:00:00 ps

└─(root㉿kali)-[~/college]
# ps -T
  PID   SPID TTY      TIME CMD
2592   2592 pts/0    00:00:06 zsh
3580   3580 pts/0    00:00:00 ps

└─(root㉿kali)-[~/college]
# ps -r
  PID TTY      STAT   TIME COMMAND
3584 pts/0    R+     0:00 ps -r

└─(root㉿kali)-[~/college]
# ps -L
  PID   LWP TTY      TIME CMD
2592   2592 pts/0    00:00:06 zsh
3589   3589 pts/0    00:00:00 ps

└─(root㉿kali)-[~/college]
# ps -eo
error: format specification must follow -o

Usage:
  ps [options]

  Try 'ps --help <simple|list|output|threads|misc|all>'
  or 'ps --help <s|l|o|t|m|a>'
  for additional help text.

For more details see ps(1).

└─(root㉿kali)-[~/college]
# ps -ax
  PID TTY      STAT   TIME COMMAND
  1 ?        Ss     0:03 /sbin/init splash
  2 ?        S      0:00 [kthreadd]
  3 ?        I<    0:00 [rcu_gp]
  4 ?        I<    0:00 [rcu_par_gp]
  6 ?        I<    0:00 [kworker/0:0H-events_highpri]
  9 ?        I<    0:00 [mm_percpu_wq]
 10 ?       S      0:00 [rcu_tasks_rude_]
 11 ?       S      0:00 [rcu_tasks_trace]

```

Top

The top command displays all the running process within the environment of your system. It helps in monitoring system usage and performances. It is mainly used to detect load on the server by system administrators.

```
(root㉿kali)-[~/college]
# top

top - 07:16:19 up 4:33, 2 users, load average: 0.07, 0.05, 0.01
Tasks: 157 total, 1 running, 156 sleeping, 0 stopped, 0 zombie
%CPU(s): 0.2 us, 0.3 sy, 0.0 ni, 99.5 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
Mem: 3000.4 total, 2083.0 free, 426.9 used, 490.5 buff/cache
Swap: 975.0 total, 975.0 free, 0.0 used. 2418.1 avail Mem

PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
 557 root      20   0 1201620 112112 44312 S  1.0  3.6  0:59.92 Xorg
2589 root      20   0 1281688 79640 63488 S  1.0  2.6  0:14.55 qterminal
 818 root      20   0 161152 2724 2224 S  0.3  0.1  0:34.54 VBoxClient
  1 root      20   0 164012 10296 7732 S  0.0  0.3  0:03.08 systemd
  2 root      20   0      0      0      0 S  0.0  0.0  0:00.03 kthreadd
  3 root      0 -20      0      0      0 I  0.0  0.0  0:00.00 rCU_gp
  4 root      0 -20      0      0      0 I  0.0  0.0  0:00.00 rCU_par_gp
  6 root      0 -20      0      0      0 I  0.0  0.0  0:00.00 kworker/0:0H-events_highpri
  9 root      0 -20      0      0      0 I  0.0  0.0  0:00.00 mm_percpu_wq
 10 root      20   0      0      0      0 S  0.0  0.0  0:00.00 rCU_tasks_rude_
 11 root      20   0      0      0      0 S  0.0  0.0  0:00.00 rCU_tasks_trace
 12 root      20   0      0      0      0 S  0.0  0.0  0:01.42 ksoftirqd/0
 13 root      20   0      0      0      0 I  0.0  0.0  0:03.07 rCU_sched
 14 root      rt   0      0      0      0 S  0.0  0.0  0:00.12 migration/0
 15 root      20   0      0      0      0 S  0.0  0.0  0:00.00 cpuhp/0
 16 root      20   0      0      0      0 S  0.0  0.0  0:00.00 cpuhp/1
 17 root      rt   0      0      0      0 S  0.0  0.0  0:00.41 migration/1
 18 root      20   0      0      0      0 S  0.0  0.0  0:00.02 ksoftirqd/1
 20 root      0 -20      0      0      0 I  0.0  0.0  0:00.00 kworker/1:0H-events_highpri
 21 root      20   0      0      0      0 S  0.0  0.0  0:00.00 cpuhp/2
 22 root      rt   0      0      0      0 S  0.0  0.0  0:00.42 migration/2
 23 root      20   0      0      0      0 S  0.0  0.0  0:00.09 ksoftirqd/2
 25 root      0 -20      0      0      0 I  0.0  0.0  0:00.00 kworker/2:0H-events_highpri
 26 root      20   0      0      0      0 S  0.0  0.0  0:00.00 cpuhp/3
 27 root      rt   0      0      0      0 S  0.0  0.0  0:00.44 migration/3
 28 root      20   0      0      0      0 S  0.0  0.0  0:00.02 ksoftirqd/3
 30 root      0 -20      0      0      0 I  0.0  0.0  0:00.00 kworker/3:0H-events_highpri
 35 root      20   0      0      0      0 S  0.0  0.0  0:00.00 kdevtmpfs
 36 root      0 -20      0      0      0 I  0.0  0.0  0:00.00 netns
 37 root      20   0      0      0      0 S  0.0  0.0  0:00.01 kauditt
 38 root      20   0      0      0      0 S  0.0  0.0  0:00.01 khungtaskd
 39 root      20   0      0      0      0 S  0.0  0.0  0:00.00 oom_reaper
 40 root      0 -20      0      0      0 I  0.0  0.0  0:00.00 writeback
 41 root      20   0      0      0      0 S  0.0  0.0  0:00.87 kcompactd0
 42 root      25   5      0      0      0 S  0.0  0.0  0:00.00 ksm
 43 root      39  19      0      0      0 S  0.0  0.0  0:00.34 khugepaged
 45 root      20   0      0      0      0 I  0.0  0.0  0:02.49 kworker/3:1-events
 62 root      0 -20      0      0      0 I  0.0  0.0  0:00.00 integrityd
 63 root      0 -20      0      0      0 I  0.0  0.0  0:00.00 kblockd
 64 root      0 -20      0      0      0 I  0.0  0.0  0:00.00 blkcg_punt_bio
 65 root      0 -20      0      0      0 I  0.0  0.0  0:00.00 edac-poller
 66 root      0 -20      0      0      0 I  0.0  0.0  0:00.00 devfreq_wq
 67 root      0 -20      0      0      0 I  0.0  0.0  0:00.06 kworker/3:1H-kblockd
 71 root      20   0      0      0      0 S  0.0  0.0  0:00.00 kswapd0
 72 root      0 -20      0      0      0 I  0.0  0.0  0:00.00 kthrotld
 73 root      0 -20      0      0      0 I  0.0  0.0  0:00.00 acpi_thermal_pm
```

WC

Linux wc command helps in counting the lines, words, and characters in a file. It displays the number of lines, number of characters, and the number of words in a file. Mostly, it is used with pipes for counting operation.

Syntax:

1. `wc [OPTION]... [FILE]...`
2. `wc [OPTION]... --files=from=F`

Options:

Some useful command line options supported by the wc command are as following:

- c, --bytes:** It is used to print the byte counts.
- m, --chars:** It is used to print the character counts.
- l, --lines:** It is used to print the newline counts.
- files=from=F:** It is used to read input from specified files.
- L, --max-line-length:** It is used to print the maximum display width.
- w, --words:** It is used to print the word counts.
- help:** It is used to display the help manual.
- version:** It is used to display the version information.

```

root@kali:~# cat > myfile.txt
helloeveryone
hope u all are fine
hai hello,helllo hi
hehe
root@kali:~# cat > myfile2.txt
hai hello
root@kali:~# wc myfile.txt
 4 10 59 myfile.txt
root@kali:~# wc myfile2.txt
 1  2 10 myfile2.txt
root@kali:~# wc -l myfile.txt
4 myfile.txt
root@kali:~# wc -w myfile.txt myfile2.txt
10 myfile.txt
 2 myfile2.txt
12 total
root@kali:~# wc -c myfile.txt
59 myfile.txt
root@kali:~# wc -m myfile.txt
59 myfile.txt

```

tar

The Linux ‘tar’ stands for tape archive, is used to create Archive and extract the Archivefiles. tar command in Linux is one of the important command which provides archiving functionality in Linux. We can use Linux tar command to create compressed or uncompressed Archive files and also maintain and modify them.

Options:

- c : Creates Archive
- x : Extract the archive
- f : creates archive with given filename
- t : displays or lists files in archived file
- u : archives and adds to an existing archive file
- v : Displays Verbose Information
- A : Concatenates the archive files
- z : zip, tells tar command that creates tar file using gzip
- j : filter archive tar file using tbzip
- W : Verify a archive file

-r : update or add file or directory in already existed .tar file

Bzip2

```
root@kali:~# ls
Desktop           f3.txt.gz    myfile2.txt.xz
Documents         f3.txt.xz    myfile.txt.gz
Downloads         file1.gz     new.tar
embedded-browser-no-sandbox.json file2.gz     Pictures
f1.txt            file3.gz     Public
f2.txt.gz          Music       Templates
f3.txt            myfile2.txt  Videos
root@kali:~# bzip2 f1.txt
root@kali:~# bzip2 -cc f3.txt > f3.txt.bz
root@kali:~# ls
Desktop           f3.txt.gz    myfile.txt.gz
Documents         f3.txt.xz    new.tar
Downloads         file1.gz     Pictures
embedded-browser-no-sandbox.json file2.gz     Public
f1.txt.bz2        file3.gz     Templates
f2.txt.gz          Music       Videos
f3.txt            myfile2.txt  myfile2.txt.xz
f3.txt.bz          myfile2.txt.xz
```

```
Desktop   embedded-browser-no-sandbox.json f3.txt    f3.txt.xz  file1.gz  Music      myfile.txt.gz  Public
Documents f1.txt                      f3.txt.bz ff1.bz2  file2.gz  myfile2.txt  new.tar    Templates
Downloads f2.txt.gz                   f3.txt.gz ff2.bz2  file3.gz  myfile2.txt.xz Pictures  Videos
root@kali:~# bzip2 -d ff1.bz2
root@kali:~# bunzip2 -c ff2.txt.bz2 > ff2.txt
bunzip2: Can't open input file ff2.txt.bz2: No such file or directory.
root@kali:~# bunzip2 -c ff2.bz2 > ff2
root@kali:~# ls
Desktop   embedded-browser-no-sandbox.json f3.txt    f3.txt.xz  ff2.bz2  file2.gz  myfile2.txt  new.tar  Templates
Documents f1.txt                      f3.txt.bz ff1      ff2.txt  file3.gz  myfile2.txt.xz Pictures  Videos
Downloads f2.txt.gz                   f3.txt.gz ff2      file1.gz  Music     myfile.txt.gz  Public
root@kali:~#
```

gzip

```
root@kali:~# apt-get install gzip
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
gzip is already the newest version (1.10-2).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@kali:~# ls
Desktop           f2.txt      new.tar
Documents         f3.txt      Pictures
Downloads         Music       Public
embedded-browser-no-sandbox.json myfile2.txt  Templates
f1.txt.gz          myfile.txt.gz Videos
root@kali:~# gzip f2.txt
root@kali:~# ls
Desktop           f2.txt.gz   new.tar
Documents         f3.txt      Pictures
Downloads         Music       Public
embedded-browser-no-sandbox.json myfile2.txt  Templates
f1.txt.gz          myfile.txt.gz Videos
root@kali:~# touch file1 file2 file3
root@kali:~# gzip file1.txt file2.txt file3.txt
gzip: file1.txt: No such file or directory
gzip: file2.txt: No such file or directory
gzip: file3.txt: No such file or directory
root@kali:~# gzip file1 file2 file3
root@kali:~# ls
Desktop           f3.txt      myfile.txt.gz
Documents         file1.gz    new.tar
Downloads         file2.gz    Pictures
embedded-browser-no-sandbox.json file3.gz    Public
f1.txt.gz          Music      Templates
```

```

root@kali:~# gzip -c f3.txt > f3.txt.gz
root@kali:~# ls
Desktop          f3.txt.gz      new.tar
Documents        file1.gz       Pictures
Downloads        file2.gz       Public
embedded-browser-no-sandbox.json file3.gz       Templates
f1.txt.gz        myfile2.txt   Videos
f2.txt.gz        myfile.txt.gz
f3.txt           myfile.txt.gz

root@kali:~# gzip -d f1.txt.gz
root@kali:~# ls
Desktop          f3.txt.gz      new.tar
Documents        file1.gz       Pictures
Downloads        file2.gz       Public
embedded-browser-no-sandbox.json file3.gz       Templates
f1.txt           myfile2.txt   Videos
f2.txt.gz        myfile.txt.gz
f3.txt           myfile.txt.gz

root@kali:~# gzip -c f2.txt > f2.txt.gz
gzip: f2.txt: No such file or directory
root@kali:~# gzip -c f2.txt.gz > f2.txt.gz
root@kali:~# ls
Desktop          f3.txt.gz      new.tar
Documents        file1.gz       Pictures
Downloads        file2.gz       Public
embedded-browser-no-sandbox.json file3.gz       Templates
f1.txt           myfile2.txt   Videos
f2.txt.gz        myfile.txt.gz
f3.txt           myfile.txt.gz

root@kali:~# █

```

XZ

```

root@kali:~# xz -d f1.txt.xz
root@kali:~# unxz -k f2.txt.xz
unxz: f2.txt.xz: No such file or directory
root@kali:~#
root@kali:~# unxz -k f3.txt.xz
unxz: f3.txt: File exists
root@kali:~# ls
Desktop          f3.txt.gz      myfile2.txt.xz
Documents        f3.txt.xz     myfile.txt.gz
Downloads        file1.gz       new.tar
embedded-browser-no-sandbox.json file2.gz       Pictures
f1.txt           file3.gz       Public
f2.txt.gz        myfile2.txt   Templates
f3.txt           myfile.txt.gz

root@kali:~# apt-get install xz-utils
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
xz-utils is already the newest version (5.2.5-1.0).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@kali:~# ls
Desktop          f3.txt.gz      new.tar
Documents        file1.gz       Pictures
Downloads        file2.gz       Public
embedded-browser-no-sandbox.json file3.gz       Templates
f1.txt           myfile2.txt   Videos
f2.txt.gz        myfile.txt.gz
f3.txt           myfile.txt.gz

root@kali:~# xz f1.txt
root@kali:~# xz -k f3.txt
root@kali:~# xz -c myfile2.txt > myfile2.txt.xz
root@kali:~# ls
Desktop          f3.txt.gz      myfile2.txt.xz
Documents        f3.txt.xz     myfile.txt.gz
Downloads        file1.gz       new.tar
embedded-browser-no-sandbox.json file2.gz       Pictures
f1.txt.xz        file3.gz       Public
f2.txt.gz        myfile2.txt   Templates
f3.txt           myfile.txt.gz

```

expr

The **expr command** is used to evaluate a given expression and display its standard output. Each separated expression is considered as an argument. These expressions could be integer and string expressions, including regular expressions. If expressions are not passed properly, it will prevent the execution of the command.

The expr command supports the following operators:

- **for integer:** addition, subtraction, multiplication, division, and modulus.
- **For strings:** regular expression, set of characters in a string.

It will be useful if we want to perform an operation while working on the terminal, such as searching for a substring in a string, searching its index, performing arithmetic operations, and more. So, the expr command allows us to perform all these tasks from the terminal.

```
[root@kali ~]
# expr 100 + 50
150

[root@kali ~]
# expr 100 - 50
50

[root@kali ~]
# expr 100 / 50
2

[root@kali ~]
# 100 \* 50
100: command not found

[root@kali ~]
# expr 100 \* 50
5000

[root@kali ~]
#
```

Redirections & Piping :

A pipe is a form of redirection to send the output of one command/program/process to another command/program/process for further processing.

Pipe is used to combine two or more commands, the output of one command acts as input to another command, and this command's output may act as input to the next command and so on.

```
#ls -l | wc -l
```

```
root@kali:~# cat /etc/myfile.txt | head -5 | tail -3
cat: /etc: Is a directory
hope u all are fine
hai hello,helllo hi
hehe
root@kali:~#
```



```
#cat /etc/passwd.txt | head -7 | tail -5
```

ssh

In Linux, ssh is a protocol, which stands for Secure Shell or Secure Socket Shell. The secure shell is useful for security while connecting to a remote server. The ssh command uses a ssh protocol, which is a secure protocol, as the data transfer between the client and the host takes place in encrypted form. It transfers the input through the client to the host and returns the output transferred by the host. It executes through TCP/IP port 22.

The encrypted connection is also used to run the commands on a Linux server, port forwarding, tunnelling, and more.

There are lots of SSH clients that are available for both commercial and free. The OpenSSH is its most widely used client. It is available for all the most used platforms such as Windows, Linux, macOS, OpenBSD, and more.

scp

- SCP (secure copy) is a command-line utility that allows you to securely
- copy files and directories between two locations.
- With scp, you can copy a file or directory:
- From your local system to a remote system.
- From a remote system to your local system.
- Between two remote systems from your local system.

- Remote file system locations are specified in format

ssh-keygen

ssh-keygen command to generate a public/private authentication key pair. Authentication keys allow a user to connect to a remote system without supplying a password. Keys must be generated for each user separately. If you generate key pairs as the root user, only the root can use the keys.

```
$ ssh-keygen -t rsa
```

ssh-copy-id

- ⊕ The ssh-copy-id command allows you to install an SSH key on a remote server's authorized keys.
- ⊕ This command facilitates SSH key login, which removes the need for a password for each login, thus ensuring a password-less, automatic login process.
- ⊕ \$ ssh-copy-id username@remote_host

```
root@kali:~# ssh --help
unknown option -- -
usage: ssh [-46AaCfGgKkMNnqsTtVvXxYy] [-B bind_interface]
           [-b bind_address] [-c cipher_spec] [-D [bind_address:]port]
           [-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]
           [-i identity_file] [-J [user@]host[:port]] [-L address]
           [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
           [-Q query_option] [-R address] [-S ctl_path] [-W host:port]
           [-w local_tun[:remote_tun]] destination [command]

[~] # ssh
usage: ssh [-46AaCfGgKkMNnqsTtVvXxYy] [-B bind_interface]
           [-b bind_address] [-c cipher_spec] [-D [bind_address:]port]
           [-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]
           [-i identity_file] [-J [user@]host[:port]] [-L address]
           [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
           [-Q query_option] [-R address] [-S ctl_path] [-W host:port]
           [-w local_tun[:remote_tun]] destination [command]

[~] # scp
usage: scp [-346ABCpqRTv] [-c cipher] [-F ssh_config] [-i identity_file]
           [-J destination] [-l limit] [-o ssh_option] [-P port]
           [-S program] source ... target

[~] # ssh root@kali
ssh: connect to host kali port 22: Connection refused

[~] # ssh -keygen
ssh: Could not resolve hostname -: Name or service not known

[~] #
```

Managing Files, Creating Users and Groups Using Command-line tools

1. a. Create six files with name of the form songX.mp3
- b. Create six files with name of the form snapX.mp3
- c. Create six files with name of the form filmX.mp3 (In each set, replace X with the numbers 1 through 6)

```

└─# cd /
[root@kali]# pwd
/
[root@kali]# ls
bin boot dev etc home initrd.img initrd.img.old lib lib32 lib64 libx32 lost+found media mnt opt proc root run sbin srv sys tmp usr var vmlinuz vmlinuz.old
[root@kali]# cd home
[root@kali]# ls
kali
[root@kali]# touch song1.mp3 song2.mp3 song3.mp3 song4.mp3 song5.mp3 song6.mp3
[root@kali]# ls
kali song1.mp3 song2.mp3 song3.mp3 song4.mp3 song5.mp3 song6.mp3
[root@kali]# touch snap1.mp3 snap2.mp3 snap3.mp3 snap4.mp3 snap5.mp3 snap6.mp3
[root@kali]# ls
kali snap1.mp3 snap2.mp3 snap3.mp3 snap4.mp3 snap5.mp3 snap6.mp3
[root@kali]# touch film1.mp3 film2.mp3 film3.mp3 film4.mp3 film5.mp3 film6.mp3
[root@kali]# ls
film1.mp3 film2.mp3 film3.mp3 film4.mp3 film5.mp3 film6.mp3
[root@kali]#

```

```

[root@kali]# touch song1.mp3 song2.mp3 song3.mp3 song4.mp3 song5.mp3 song6.mp3
[root@kali]# ls
kali song1.mp3 song2.mp3 song3.mp3 song4.mp3 song5.mp3 song6.mp3
[root@kali]# touch snap1.mp3 snap2.mp3 snap3.mp3 snap4.mp3 snap5.mp3 snap6.mp3
[root@kali]# ls
kali snap1.mp3 snap2.mp3 snap3.mp3 snap4.mp3 snap5.mp3 snap6.mp3
[root@kali]# touch film1.mp3 film2.mp3 film3.mp3 film4.mp3 film5.mp3 film6.mp3
[root@kali]# ls
film1.mp3 film2.mp3 film3.mp3 film4.mp3 film5.mp3 film6.mp3
[root@kali]#

```

2.From your home directory, move the song files into your music subdirectory, the snapshot files into your picturesubdirectory, and the movie files into videos subdirectory.

```
(root㉿kali)-[~/home]
# mv -v song1.mp3 /root/Music
renamed 'song1.mp3' → '/root/Music/song1.mp3'
(root㉿kali)-[~/home]
# ls
film1.mp3 film2.mp3 film3.mp3 film4.mp3 film5.mp3 film6.mp3 kali snap1.mp3 snap2.mp3 snap3.mp3 snap4.mp3 snap5.mp3 snap6.mp3 song2.mp3 song3.mp3 song4.mp3 song5.mp3 song6.mp3
(root㉿kali)-[~/home]
# cd /
(boot㉿kali)-[~]
# cd root
(boot㉿kali)-[~]
# cd music
cd: no such file or directory: music
(boot㉿kali)-[~]
# cd Music
(boot㉿kali)-[~/Music]
# ls
```



```
(root㉿kali)-[~/home]
# mv -v song2.mp3 song3.mp3 song4.mp3 song5.mp3 song6.mp3 /root/Music
renamed 'song2.mp3' → '/root/Music/song2.mp3'
renamed 'song3.mp3' → '/root/Music/song3.mp3'
renamed 'song4.mp3' → '/root/Music/song4.mp3'
renamed 'song5.mp3' → '/root/Music/song5.mp3'
renamed 'song6.mp3' → '/root/Music/song6.mp3'

(boot㉿kali)-[~/home]
# cd /
(boot㉿kali)-[~]
# cd root
(boot㉿kali)-[~]
# cd music
cd: no such file or directory: music
(boot㉿kali)-[~]
# cd Music
(boot㉿kali)-[~/Music]
# ls
college song1.mp3 song2.mp3 song3.mp3 song4.mp3 song5.mp3 song6.mp3
(boot㉿kali)-[~/Music]
#
```

```
└──(root💀 kali)-[~/]
└─# cd home

└──(root💀 kali)-[/home]
└─# mv -v film1.mp3 /root/Videos
renamed 'film1.mp3' → '/root/Videos/film1.mp3'

└──(root💀 kali)-[/home]
└─# mv -v film2.mp3 film3.mp3 film4.mp3 film5.mp3 film6.mp3 root/Videos
mv: target 'root/Videos' is not a directory

└──(root💀 kali)-[/home]
└─# mv -v film2.mp3 film3.mp3 film4.mp3 film5.mp3 film6.mp3 /root/Videos
renamed 'film2.mp3' → '/root/Videos/film2.mp3'
renamed 'film3.mp3' → '/root/Videos/film3.mp3'
renamed 'film4.mp3' → '/root/Videos/film4.mp3'
renamed 'film5.mp3' → '/root/Videos/film5.mp3'
renamed 'film6.mp3' → '/root/Videos/film6.mp3'

└──(root💀 kali)-[/home]
└─# cd ..

└──(root💀 kali)-[~]
└─# cd Videos

└──(root💀 kali)-[~/Videos]
└─# ls
film1.mp3  film2.mp3  film3.mp3  film4.mp3  film5.mp3  film6.mp3

└──(root💀 kali)-[~/Videos]
└─# █
```

```
(root💀 kali)-[~/home]
└─# mv -v snap1.mp3 snap2.mp3 snap3.mp3 snap4.mp3 snap5.mp3 snap6.mp3 /root/Pictures
renamed 'snap1.mp3' → '/root/Pictures/snap1.mp3'
renamed 'snap2.mp3' → '/root/Pictures/snap2.mp3'
renamed 'snap3.mp3' → '/root/Pictures/snap3.mp3'
renamed 'snap4.mp3' → '/root/Pictures/snap4.mp3'
renamed 'snap5.mp3' → '/root/Pictures/snap5.mp3'
renamed 'snap6.mp3' → '/root/Pictures/snap6.mp3'

(root💀 kali)-[~/home]
└─# cd ↵

(root💀 kali)-[~]
└─# cd Pictures

(root💀 kali)-[~/Pictures]
└─# ls
snap1.mp3  snap2.mp3  snap3.mp3  snap4.mp3  snap5.mp3  snap6.mp3

(root💀 kali)-[~/Pictures]
└─# █
```

3. In your home directory, create three subdirectories for organizing your files. Call these directories friends, family, and work. Create all three with one command

```
(root💀 kali)-[~/Pictures]
└─# cd ↵

(root💀 kali)-[~]
└─# cd home

(root💀 kali)-[/home]
└─# ls
kali

(root💀 kali)-[/home]
└─# mkdir friends family work

(root💀 kali)-[/home]
└─# ls
family  friends  kali  work

(root💀 kali)-[/home]
└─# █
```

4. Copy song files to the friends folder and snap files to family folder

```
[root💀 kali]-(~/Music)
# cp song1.mp3 song2.mp3 song3.mp3 song4.mp3 song5.mp3 song6.mp3 /home/friends

[root💀 kali]-(~/Music)
# cd ..

[root💀 kali]-[/]
# cd home

[root💀 kali]-[/home]
# cd friends

[root💀 kali]-[/home/friends]
# ls
song1.mp3  song2.mp3  song3.mp3  song4.mp3  song5.mp3  song6.mp3

[root💀 kali]-[/home/friends]
# 
```

```
[root💀 kali]-[~/Pictures]
# cp snap1.mp3 snap2.mp3 snap3.mp3 snap4.mp3 snap5.mp3 snap6.mp3 /home/family

[root💀 kali]-[~/Pictures]
# cd ..

[root💀 kali]-[/]
# cd home

[root💀 kali]-[/home]
# cd family

[root💀 kali]-[/home/family]
# ls
snap1.mp3  snap2.mp3  snap3.mp3  snap4.mp3  snap5.mp3  snap6.mp3

[root💀 kali]-[/home/family]
# 
```

5. Attempt to delete both family and friends projects with a single rmdir command.

```
[root@kali ~]# rmdir friends family
[root@kali ~]# ls
allfiles.txt  kali  song1.mp3  work
[root@kali ~]#
```

6. Use another command that will succeed in deleting both the family and friends folder.

```
[root@kali ~]# rm -r friends family
[root@kali ~]# ls
kali  song1.mp3  work
[root@kali ~]#
```

7. Redirect a long listing of all home directory files, including hidden, into a file named allfiles.txt. Confirm that thefile contains the listing.

```
[root@kali ~]# ls -a > allfiles.txt
[root@kali ~]# ls
allfiles.txt  family  friends  kali  song1.mp3  work
[root@kali ~]
```

8.In the command window, display today's date with day of the week month, date and year

```
[root💀kali]-[~/home]
# date
Tue 17 Aug 2021 07:27:57 AM EDT

[root💀kali]-[~/home]
#
```

9Add the user Juliet

```
[root💀 kali]~$ useradd Juliet  
[root💀 kali]~$ passwd Juliet  
New password:  
Retype new password:  
passwd: password updated successfully  
[root💀 kali]~$
```

10.Confirm that Juliet has been added by examining the /etc/passwd file

```
[root💀 kali]~$ cat /etc/passwd | grep Juliet  
Juliet:x:1003:1005::/home/Juliet:/bin/sh
```

11.Use the passwd command to initialize Juliet's password

```
[root💀 kali]~$ useradd Juliet  
[root💀 kali]~$ passwd Juliet  
New password:  
Retype new password:  
passwd: password updated successfully  
[root💀 kali]~$
```

12. Create a supplementary group called Shakespeare with a group id of 30000

```
[root💀 kali] ~
# groupadd -g 30000 Shakespeare
[root💀 kali] ~
#
```

5. Create a supplementary group called artists.

```
[root💀 kali] ~
# groupadd artists
```

6. Confirm that Shakespeare and artists have been added by examining the /etc/group file.

```
[root💀 kali] ~
# less /etc/group
zsh: suspended less /etc/group
```

```
kali-trusted:x:122:  
postgres:x:123:  
i2c:x:124:  
avahi:x:125:  
stunnel4:x:126:  
Debian-snmp:x:127:  
sslh:x:128:  
nm-openvpn:x:129:  
nm-openconnect:x:130:  
pulse:x:131:  
pulse-access:x:132:  
scanner:x:133:saned,kali  
saned:x:134:  
sambashare:x:135:  
inetsim:x:136:  
colord:x:137:  
geoclue:x:138:  
lightdm:x:139:  
kpadmins:x:140:  
kali:x:1000:  
vboxsf:x:141:  
kaboxer:x:142:kali,root  
systemd-coredump:x:999:  
nbin:x:1001:  
test_user:x:1002:  
groupname:x:1003:  
usrgrp:x:1004:  
Juliet:x:1005:  
Shakespheare:x:30000:  
artists:x:30001:  
(END)
```

7. Add the Juliet user to the Shakespeare group as a supplementary group.

```
[root@kali] ~]  
# usermod -G Shakespeare Juliet
```

8. Confirm that Juliet has been added using the id command.

```
[root@kali] ~]  
# id Juliet  
uid=1003(Juliet) gid=1005(Juliet) groups=1005(Juliet),30000(Shakespeare)  
[root@kali] ~]  
#
```

9. Add Romeo and Hamlet to the Shakespeare group.

```
[root💀 kali]~# useradd Romeo
[root💀 kali]~# useradd hamlet
[root💀 kali]~# usermod -G Shakespeare Romeo
[root💀 kali]~# usermod -G Shakespeare Hamlet
usermod: user 'Hamlet' does not exist
[root💀 kali]~# usermod -G Shakespeare hamlet
[root💀 kali]~#
```

10. Add Reba, Dolly and Elvis to the artists group

```
[~] (root㉿kali)-[~]
└─# useradd Reba

[~] (root㉿kali)-[~]
└─# useradd Dolly

[~] (root㉿kali)-[~]
└─# useradd Elvis

[~] (root㉿kali)-[~]
└─# usermod -G artists Reba

[~] (root㉿kali)-[~]
└─# usermod -G artists Dolly

[~] (root㉿kali)-[~]
└─# usermod -G artists Elvis

[~] (root㉿kali)-[~]
└─#
```

11. Verify the supplemental group memberships by examining the /etc/group file

```
[~] (root㉿kali)-[~]
└─# less /etc/group
zsh: suspended less /etc/group
[~] (root㉿kali)-[~]
└─# less /etc/group
usrgrp:x:1004:
Juliet:x:1005:
Shakespeare:x:30000:Juliet,Romeo,hamlet
artists:x:30001:Reba,Dolly,Elvis
Romeo:x:30002:
hamlet:x:30003:
Reba:x:1006:
Dolly:x:1007:
Elvis:x:1008:
(END)
```

12. Attempt to remove user Dolly.

```
[root💀kali]-[~]
└─# userdel Dolly

[root💀kali]-[~]
└─# less /etc/group

zsh: suspended less /etc/group

[root💀kali]-[~]
└─# █
```

```
usrgrp:x:1004:
Juliet:x:1005:
Shakespheare:x:30000:Juliet,Romeo,hamlet
artists:x:30001:Reba,Elvis
Romeo:x:30002:
hamlet:x:30003:
Reba:x:1006:
Elvis:x:1008:
```

1.Ping & traceroute tests

Ping and Trace Route tests can help to identify any connection issues between your network and a specified server (or website) address.

PING test

The PING command is used to test the connection and latency between two network connections. The PING command sends packets of information to a specified IP Address and then measures the time it takes to get a response from the specified computer or device.

Trace Route test

The TRACERT command is used to conduct a similar test to PING, but instead of displaying the time it takes to connect, it looks at the exact server hops required to connect your computer to the server. You should already have the CMD prompt dialogue box open, after performing the PING test above.

```
Microsoft Windows [Version 10.0.19043.1202]
(c) Microsoft Corporation. All rights reserved.

C:\Users\nibin>ping www.google.com

Pinging www.google.com [142.250.77.164] with 32 bytes of data:
Reply from 142.250.77.164: bytes=32 time=112ms TTL=119
Reply from 142.250.77.164: bytes=32 time=21ms TTL=119
Reply from 142.250.77.164: bytes=32 time=24ms TTL=119
Reply from 142.250.77.164: bytes=32 time=22ms TTL=119

Ping statistics for 142.250.77.164:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 21ms, Maximum = 112ms, Average = 44ms

C:\Users\nibin>tracert www.google.com

Tracing route to www.google.com [142.250.77.164]
over a maximum of 30 hops:

 1    72 ms    101 ms      3 ms  192.168.1.1
 2      6 ms       6 ms      6 ms  100.77.128.1
 3    33 ms    23 ms     27 ms  10.1.3.6
 4   120 ms    101 ms    101 ms  72.14.212.92
 5     22 ms     25 ms     22 ms  216.239.54.67
 6   106 ms    106 ms     94 ms  209.85.142.247
 7   134 ms    100 ms    101 ms  maa05s17-in-f4.1e100.net [142.250.77.164]

Trace complete.

C:\Users\nibin>
```

1.Nslookup

Microsoft Windows includes a tool called NSLOOKUP that you can use via the command prompt. This tool can be used to check DNS records propagation and resolution using different servers, and perform other troubleshooting steps.

```
C:\Users\nibin>nslookup aesajce.com
Server:  UnKnown
Address: 103.140.17.242
```

- Type nslookup -q=XX where XX is a type of a DNS record. Some of the available types are MX, A, CNAME, and TXT. The records are then displayed, to exit the tool type exit
- To use **nslookup** as a troubleshooting tool, you can set the specific type of record to lookup for a domain by using the **-type=record_type** where **record_type** is A, CNAME, MX, PTR, NS, ANY.
Type **nslookup -type=ns domain_name** where **domain_name** is the domain for your query and hit **Enter**. Now the tool will display the name servers for the domain you specified.

```
C:\Users\nibin>nslslookup google.com
Server: UnKnown
Address: 103.140.17.242

Non-authoritative answer:
Name: google.com
Addresses: 2404:6800:4007:82b::200e
           142.250.196.46

C:\Users\nibin>nslslookup -q=wX google.com
unknown query type: WX
Server: UnKnown
Address: 103.140.17.242

Non-authoritative answer:
DNS request timed out.
    timeout was 2 seconds.
Name: google.com
Address: 142.250.196.46

C:\Users\nibin>nslslookup -type=ns google.com
Server: UnKnown
Address: 103.140.17.242

Non-authoritative answer:
google.com      nameserver = ns3.google.com
google.com      nameserver = ns4.google.com
google.com      nameserver = ns1.google.com
google.com      nameserver = ns2.google.com
```

2. Netstat

On Windows 10, netstat (network statistics) has been around for a long time, and it's a command-line tool that you can use in Command Prompt to display statistics for all network connections. It allows you to understand open and connected ports to monitor and troubleshoot networking problems for system or applications.

```
C:\Users\nibin>netstat
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49669        LAPTOP-8MQED7V9:49670 ESTABLISHED
  TCP    127.0.0.1:49670        LAPTOP-8MQED7V9:49669 ESTABLISHED
  TCP    127.0.0.1:49671        LAPTOP-8MQED7V9:49672 ESTABLISHED
  TCP    127.0.0.1:49672        LAPTOP-8MQED7V9:49671 ESTABLISHED
  TCP    127.0.0.1:49674        LAPTOP-8MQED7V9:49675 ESTABLISHED
  TCP    127.0.0.1:49675        LAPTOP-8MQED7V9:49674 ESTABLISHED
  TCP    127.0.0.1:49676        LAPTOP-8MQED7V9:49677 ESTABLISHED
  TCP    127.0.0.1:49677        LAPTOP-8MQED7V9:49676 ESTABLISHED
  TCP    127.0.0.1:49678        LAPTOP-8MQED7V9:49679 ESTABLISHED
  TCP    127.0.0.1:49679        LAPTOP-8MQED7V9:49678 ESTABLISHED
  TCP    127.0.0.1:49680        LAPTOP-8MQED7V9:49681 ESTABLISHED
  TCP    127.0.0.1:49681        LAPTOP-8MQED7V9:49680 ESTABLISHED
  TCP    127.0.0.1:49682        LAPTOP-8MQED7V9:49683 ESTABLISHED
  TCP    127.0.0.1:49683        LAPTOP-8MQED7V9:49682 ESTABLISHED
  TCP    127.0.0.1:49684        LAPTOP-8MQED7V9:49685 ESTABLISHED
  TCP    127.0.0.1:49685        LAPTOP-8MQED7V9:49684 ESTABLISHED
  TCP    127.0.0.1:49686        LAPTOP-8MQED7V9:49687 ESTABLISHED
  TCP    127.0.0.1:49687        LAPTOP-8MQED7V9:49686 ESTABLISHED
  TCP    127.0.0.1:49688        LAPTOP-8MQED7V9:49689 ESTABLISHED
  TCP    127.0.0.1:49689        LAPTOP-8MQED7V9:49688 ESTABLISHED
  TCP    192.168.1.5:50048       20.198.162.78:https ESTABLISHED
  TCP    192.168.1.5:50057       maa05s13-in-f1:https TIME_WAIT
  TCP    192.168.1.5:52895       maa03s43-in-f14:https ESTABLISHED
  TCP    192.168.1.5:53300       117.18.237.29:http CLOSE_WAIT
  TCP    192.168.1.5:53417       sf-in-f188:5228 ESTABLISHED
  TCP    192.168.1.5:55115       maa03s38-in-f22:https ESTABLISHED
  TCP    192.168.1.5:55320       59:https ESTABLISHED
  TCP    192.168.1.5:59410       75:https ESTABLISHED
  TCP    192.168.1.5:60242       maa05s09-in-f3:https TIME_WAIT
  TCP    192.168.1.5:60243       20.190.146.34:https TIME_WAIT
  TCP    192.168.1.5:60244       20.189.173.3:https TIME_WAIT
  TCP    192.168.1.5:60246       20.198.162.78:https ESTABLISHED
  TCP    192.168.1.5:60247       219:https ESTABLISHED
  TCP    192.168.1.5:60338       85:https ESTABLISHED
  TCP    192.168.1.5:60675       maa03s38-in-f22:https TIME_WAIT
  TCP    192.168.1.5:60820       219:https TIME_WAIT
  TCP    192.168.1.5:60938       maa03s28-in-f2:https TIME_WAIT
  TCP    192.168.1.5:60939       40.126.17.133:https ESTABLISHED
  TCP    192.168.1.5:63960       dns:https CLOSE_WAIT
  TCP    192.168.1.5:64579       s3-us-west-2-r-w:https CLOSE_WAIT
  TCP    192.168.1.5:64580       s3-us-west-2-r-w:https CLOSE_WAIT
```

netstat -n

command to display active connections showing numeric IP address and port number instead of trying to determine the names .

netstat -n INTERVAL

In the command, make sure to replace INTERVAL for the number (in seconds) you want to redisplay the information.

Active Connections			
Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:49669	127.0.0.1:49670	ESTABLISHED
TCP	127.0.0.1:49670	127.0.0.1:49669	ESTABLISHED
TCP	127.0.0.1:49671	127.0.0.1:49672	ESTABLISHED
TCP	127.0.0.1:49672	127.0.0.1:49671	ESTABLISHED
TCP	127.0.0.1:49674	127.0.0.1:49675	ESTABLISHED
TCP	127.0.0.1:49675	127.0.0.1:49674	ESTABLISHED
TCP	127.0.0.1:49676	127.0.0.1:49677	ESTABLISHED
TCP	127.0.0.1:49677	127.0.0.1:49676	ESTABLISHED
TCP	127.0.0.1:49678	127.0.0.1:49679	ESTABLISHED
TCP	127.0.0.1:49679	127.0.0.1:49678	ESTABLISHED
TCP	127.0.0.1:49680	127.0.0.1:49681	ESTABLISHED
TCP	127.0.0.1:49681	127.0.0.1:49680	ESTABLISHED
TCP	127.0.0.1:49682	127.0.0.1:49683	ESTABLISHED
TCP	127.0.0.1:49683	127.0.0.1:49682	ESTABLISHED
TCP	127.0.0.1:49684	127.0.0.1:49685	ESTABLISHED
TCP	127.0.0.1:49685	127.0.0.1:49684	ESTABLISHED
TCP	127.0.0.1:49686	127.0.0.1:49687	ESTABLISHED
TCP	127.0.0.1:49687	127.0.0.1:49686	ESTABLISHED
TCP	127.0.0.1:49688	127.0.0.1:49689	ESTABLISHED
TCP	127.0.0.1:49689	127.0.0.1:49688	ESTABLISHED
TCP	192.168.1.5:49442	142.250.195.86:443	TIME_WAIT
TCP	192.168.1.5:49445	52.98.59.18:443	ESTABLISHED
TCP	192.168.1.5:49448	117.18.232.200:443	CLOSE_WAIT
TCP	192.168.1.5:49449	13.107.246.254:443	ESTABLISHED
TCP	192.168.1.5:49450	204.79.197.222:443	ESTABLISHED
TCP	192.168.1.5:49451	40.126.17.133:443	ESTABLISHED
TCP	192.168.1.5:49468	142.250.196.78:443	ESTABLISHED
TCP	192.168.1.5:50048	20.198.162.78:443	ESTABLISHED
TCP	192.168.1.5:52895	142.250.195.238:443	TIME_WAIT
TCP	192.168.1.5:53292	142.250.196.66:443	ESTABLISHED
TCP	192.168.1.5:53417	74.125.24.188:5228	ESTABLISHED
TCP	192.168.1.5:53837	142.250.67.65:443	ESTABLISHED
TCP	192.168.1.5:53838	35.247.144.219:443	ESTABLISHED
TCP	192.168.1.5:55320	35.201.104.59:443	ESTABLISHED
TCP	192.168.1.5:59546	142.250.195.86:443	ESTABLISHED
TCP	192.168.1.5:60246	20.198.162.78:443	ESTABLISHED
TCP	192.168.1.5:60338	35.201.97.85:443	ESTABLISHED
TCP	192.168.1.5:63157	8.8.8.8:443	ESTABLISHED
TCP	192.168.1.5:64579	52.218.181.193:443	CLOSE_WAIT
TCP	192.168.1.5:64580	52.218.224.73:443	CLOSE_WAIT

netstat -a

The netstat -a command displays all active and inactive connections, and the TCP and UDP ports the device is currently listening.

```
C:\Users\nibin>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135           LAPTOP-8MQED7V9:0   LISTENING
  TCP    0.0.0.0:445           LAPTOP-8MQED7V9:0   LISTENING
  TCP    0.0.0.0:3306          LAPTOP-8MQED7V9:0   LISTENING
  TCP    0.0.0.0:5040          LAPTOP-8MQED7V9:0   LISTENING
  TCP    0.0.0.0:6646          LAPTOP-8MQED7V9:0   LISTENING
  TCP    0.0.0.0:33060         LAPTOP-8MQED7V9:0   LISTENING
  TCP    0.0.0.0:49664         LAPTOP-8MQED7V9:0   LISTENING
  TCP    0.0.0.0:49665         LAPTOP-8MQED7V9:0   LISTENING
  TCP    0.0.0.0:49666         LAPTOP-8MQED7V9:0   LISTENING
  TCP    0.0.0.0:49667         LAPTOP-8MQED7V9:0   LISTENING
  TCP    0.0.0.0:49668         LAPTOP-8MQED7V9:0   LISTENING
  TCP    0.0.0.0:49673         LAPTOP-8MQED7V9:0   LISTENING
  TCP    127.0.0.1:27017       LAPTOP-8MQED7V9:0   LISTENING
  TCP    127.0.0.1:49669       LAPTOP-8MQED7V9:49670 ESTABLISHED
  TCP    127.0.0.1:49670       LAPTOP-8MQED7V9:49669 ESTABLISHED
  TCP    127.0.0.1:49671       LAPTOP-8MQED7V9:49672 ESTABLISHED
  TCP    127.0.0.1:49672       LAPTOP-8MQED7V9:49671 ESTABLISHED
  TCP    127.0.0.1:49674       LAPTOP-8MQED7V9:49675 ESTABLISHED
  TCP    127.0.0.1:49675       LAPTOP-8MQED7V9:49674 ESTABLISHED
  TCP    127.0.0.1:49676       LAPTOP-8MQED7V9:49677 ESTABLISHED
  TCP    127.0.0.1:49677       LAPTOP-8MQED7V9:49676 ESTABLISHED
  TCP    127.0.0.1:49678       LAPTOP-8MQED7V9:49679 ESTABLISHED
  TCP    127.0.0.1:49679       LAPTOP-8MQED7V9:49678 ESTABLISHED
  TCP    127.0.0.1:49680       LAPTOP-8MQED7V9:49681 ESTABLISHED
  TCP    127.0.0.1:49681       LAPTOP-8MQED7V9:49680 ESTABLISHED
  TCP    127.0.0.1:49682       LAPTOP-8MQED7V9:49683 ESTABLISHED
  TCP    127.0.0.1:49683       LAPTOP-8MQED7V9:49682 ESTABLISHED
  TCP    127.0.0.1:49684       LAPTOP-8MQED7V9:49685 ESTABLISHED
  TCP    127.0.0.1:49685       LAPTOP-8MQED7V9:49684 ESTABLISHED
  TCP    127.0.0.1:49686       LAPTOP-8MQED7V9:49687 ESTABLISHED
  TCP    127.0.0.1:49687       LAPTOP-8MQED7V9:49686 ESTABLISHED
  TCP    127.0.0.1:49688       LAPTOP-8MQED7V9:49689 ESTABLISHED
  TCP    127.0.0.1:49689       LAPTOP-8MQED7V9:49688 ESTABLISHED
  TCP    192.168.1.5:139        LAPTOP-8MQED7V9:0   LISTENING
  TCP    192.168.1.5:49235      maa03s29-in-f1:https ESTABLISHED
```

netstat -b

The netstat -b command lists all the executables (applications) associated with each connection. Sometimes, applications may open multiple connections.

netstat -e

The netstat -e command generates a statistic of the network interface, which shows information like the number of bytes, unicast and non-unicast sent and received packets. You can also see discarded packets and errors and unknown protocols, which can you troubleshoot networking problems.

```
Microsoft Windows [Version 10.0.19043.1202]
(c) Microsoft Corporation. All rights reserved.

C:\Users\nibin>netstat -b
The requested operation requires elevation.

C:\Users\nibin>netstat -e
Interface Statistics

Received          Sent
Bytes            2973437600      154413434
Unicast packets   3309502        1126251
Non-unicast packets  9149        27741
Discards          0              0
Errors            0              0
Unknown protocols 0              0

C:\Users\nibin>
```

1. ipconfig

Displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. Used without parameters, ipconfig displays Internet Protocol version 4 (IPv4) and IPv6 addresses, subnet mask, and default gateway for all adapters.

PARAMETERS:

/all: Displays the full TCP/IP configuration for all adapters. Adapters can represent physical interfaces, such as installed network adapters, or logical interfaces, such as dial-up connections.

/displaydns: Displays the contents of the DNS client resolver cache, which includes both entries preloaded from the local Hosts file and any recently obtained resource records name

queries resolved by the computer. The DNS Client service uses this information to resolve frequently queried names quickly, before querying its configured DNS servers.

/flushdns: Flushes and resets the contents of the DNS client resolver cache. During DNS troubleshooting, you can use this procedure to discard negative cache entries from the cache, as well as any other entries that have been added dynamically.

/registerdns: Initiates manual dynamic registration for the DNS names and IP addresses that are configured at a computer. You can use this parameter to troubleshoot a failed DNS name registration or resolve a dynamic update problem between a client and the DNS server without rebooting the client computer. The DNS settings in the advanced properties of the TCP/IP protocol determine which names are registered in DNS.

```
C:\Users\nibin>ipconfig
Windows IP Configuration

Ethernet adapter VirtualBox Host-Only Network:
  Connection-specific DNS Suffix . . . . . : fe80::5:87d5:7110:3e18%12
  Link-local IPv6 Address . . . . . : 192.168.56.1
  IPv4 Address . . . . . : 255.255.255.0
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :

Wireless LAN adapter Local Area Connection* 1:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . :
  Wireless LAN adapter Local Area Connection* 2:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . :
  Wireless LAN adapter Wi-Fi:
    Connection-specific DNS Suffix . . . . . : fe80::7d1f:3fa:4729:cfb1%16
    Link-local IPv6 Address . . . . . : 192.168.1.5
    IPv4 Address . . . . . : 255.255.255.0
    Subnet Mask . . . . . : 192.168.1.1
    Default Gateway . . . . . :

Ethernet adapter Bluetooth Network Connection:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . :

C:\Users\nibin>ipconfig /all
Windows IP Configuration

  Host Name . . . . . : LAPTOP-8MQED7V9
  Primary Dns Suffix . . . . . :
  Node Type . . . . . : Hybrid
  IP Routing Enabled. . . . . : No
  WINS Proxy Enabled. . . . . : No

Ethernet adapter VirtualBox Host-Only Network:
  Connection-specific DNS Suffix . . . . . : VirtualBox Host-Only Ethernet Adapter
  Description . . . . . : VirtualBox Host-Only Ethernet Adapter
  Physical Address . . . . . : 0A-00-27-00-00-0C
  DHCP Enabled. . . . . : No
```

```
NetBIOS over Tcpip. . . . . : Enabled  
TENZI0.0.0.11111.5701  
Wireless LAN adapter Local Area Connection* 1:  
Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix . . . . .  
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter  
Physical Address . . . . . : DA-C0-A6-9B-65-FF  
DHCP Enabled. . . . . : Yes  
Autoconfiguration Enabled . . . . . : Yes  
Wireless LAN adapter Local Area Connection* 2:  
Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix . . . . .  
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2  
Physical Address . . . . . : D8-C0-A6-9B-65-FF  
DHCP Enabled. . . . . : Yes  
Autoconfiguration Enabled . . . . . : Yes  
Wireless LAN adapter Wi-Fi:  
Connection-specific DNS Suffix . . . . .  
Description . . . . . : Realtek RTL8723DE 802.11b/g/n PCIe Adapter  
Physical Address . . . . . : D8-C0-A6-9B-65-FF  
DHCP Enabled. . . . . : Yes  
Autoconfiguration Enabled . . . . . : Yes  
Link-local IPv6 Address . . . . . : fe80::7d1f:3fa:4729:cfb1%16(PREFERRED)  
IPv4 Address. . . . . : 192.168.1.5(PREFERRED)  
Subnet Mask . . . . . : 255.255.255.0  
Lease Obtained. . . . . : 13 September 2021 18:56:37  
Lease Expires . . . . . : 14 September 2021 18:56:37  
Default Gateway . . . . . : 192.168.1.1  
DHCP Server . . . . . : 192.168.1.1  
DHCPv6 IAID . . . . . : 148422822  
DHCPv6 Client DUID. . . . . : 00-01-00-01-27-37-1A-F8-9C-EB-E8-9F-64-69  
DNS Servers . . . . . : 103.140.17.242  
8.8.8.8  
NetBIOS over Tcpip. . . . . : Enabled  
Ethernet adapter Bluetooth Network Connection:  
Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix . . . . .  
Description . . . . . : Bluetooth Device (Personal Area Network)  
Physical Address . . . . . : D8-C0-A6-9B-65-FE  
DHCP Enabled. . . . . : Yes  
Autoconfiguration Enabled . . . . . : Yes  
c:\Users\nibin>
```

Other Networking Commands

1. Hostname Command

A very simple command that displays the host name of your machine. This is much quicker than going to the control panel>system route.

2. getmac Command

Another very simple command that shows the MAC address of your network interfaces

3. arp Command

This is used for showing the address resolution cache. This command must be used with a command line switch arp -a is the most common.

4. Nbtstat

Diagnostic tool for troubleshooting netBIOS problems.

5. Net Command

Used for managing users, service, shares etc..

```
Microsoft Windows [Version 10.0.19043.1202]
(c) Microsoft Corporation. All rights reserved.

C:\Users\nibin>net
The syntax of this command is:

NET
[ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
HELPMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
STATISTICS | STOP | TIME | USE | USER | VIEW ]

C:\Users\nibin>D:
D:\>net
The syntax of this command is:

NET
[ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
HELPMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
STATISTICS | STOP | TIME | USE | USER | VIEW ]

D:\>
```

```
D:\>nbtstat  
Displays protocol statistics and current TCP/IP connections using NBT  
(NetBIOS over TCP/IP).  
NBTSTAT [ [-a RemoteName] [-A IP address] [-c] [-n]  
[-r] [-R] [-RR] [-s] [-S] [interval] ]  
-a (adapter status) Lists the remote machine's name table given its name  
-A (Adapter status) Lists the remote machine's name table given its  
IP address.  
-c (cache) Lists NBT's cache of remote [machine] names and their IP addresses  
-n (names) Lists local NetBIOS names.  
-r (resolved) Lists names resolved by broadcast and via WINS  
-R (Reload) Purges and reloads the remote cache name table  
-S (Sessions) Lists sessions table with the destination IP addresses  
-s (sessions) Lists sessions table converting destination IP  
addresses to computer NETBIOS names.  
-RR (ReleaseRefresh) Sends Name Release packets to WINS and then, starts Refresh  
  
RemoteName Remote host machine name.  
IP address Dotted decimal representation of the IP address.  
interval Redisplays selected statistics, pausing interval seconds  
between each display. Press Ctrl+C to stop redisplaying  
statistics.
```

```
D:\>
```

ping

```
[user@parrot] -[~] $ ping google.com
PING google.com (142.250.196.78) 56(84) bytes of data.
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=1 ttl=119 time=22.7 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=2 ttl=119 time=22.4 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=3 ttl=119 time=21.4 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=4 ttl=119 time=21.5 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=5 ttl=119 time=21.7 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=6 ttl=119 time=20.8 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=7 ttl=119 time=21.3 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=8 ttl=119 time=21.1 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=9 ttl=119 time=21.5 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=10 ttl=119 time=21.6 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=11 ttl=119 time=22.8 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=12 ttl=119 time=101 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=13 ttl=119 time=21.1 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=14 ttl=119 time=21.5 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=15 ttl=119 time=22.2 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=16 ttl=119 time=20.8 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=17 ttl=119 time=21.8 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=18 ttl=119 time=21.3 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=19 ttl=119 time=33.7 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=20 ttl=119 time=20.8 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=21 ttl=119 time=21.6 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=22 ttl=119 time=22.7 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=23 ttl=119 time=22.1 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=24 ttl=119 time=23.6 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=25 ttl=119 time=20.7 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=26 ttl=119 time=21.7 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=27 ttl=119 time=21.7 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=28 ttl=119 time=21.3 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=29 ttl=119 time=21.1 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=30 ttl=119 time=22.9 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=31 ttl=119 time=22.2 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=32 ttl=119 time=22.6 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=33 ttl=119 time=23.1 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=34 ttl=119 time=20.8 ms
```


Route

```
[x]-[user@parrot]-[~]
└─$ route
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref    Use Iface
default         192.168.1.1   0.0.0.0       UG    100    0        0 eth0
192.168.1.0    0.0.0.0       255.255.255.0 U      100    0        0 eth0
[~]
└─$ route -n
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref    Use Iface
0.0.0.0         192.168.1.1   0.0.0.0       UG    100    0        0 eth0
192.168.1.0    0.0.0.0       255.255.255.0 U      100    0        0 eth0
[~]
└─$ route -Cn
Kernel IP routing cache
Source          Destination     Gateway        Flags Metric Ref    Use Iface
[~]
└─$ ip route
default via 192.168.1.1 dev eth0 proto dhcp metric 100
192.168.1.0/24 dev eth0 proto kernel scope link src 192.168.1.8 metric 100
[~]
└─$
```

Traceroute

```
[x]-[user@parrot]-[~] $traceroute google.com
traceroute to google.com (142.250.196.78), 30 hops max, 60 byte packets
1 192.168.1.1 (192.168.1.1) 3.838 ms 4.853 ms 7.310 ms
2 * * *
3 * * *
4 * * *
5 * * *
6 * * *
7 * * *WORD.txt
8 * * *
9 * * *
10 * * *
11 * * *
12 * * *
13 * * *
14 * * *
15 * * Tish
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *
```

```
[x]-[user@parrot]-[~] $traceroute -d google.com
traceroute to google.com (142.250.196.78), 30 hops max, 60 byte packets
setsockopt SO_DEBUG: Permission denied
[x]-[user@parrot]-[~] $
```

Nslookup

```
[user@parrot]~]$ traceroute -d google.com
traceroute to google.com (142.250.196.78), 30 hops max, 60 byte packets
setsockopt SO_DEBUG: Permission denied
[x]~[user@parrot]~]$ nslookup google.com
Server: 103.140.17.242
Address: 103.140.17.242#53

Non-authoritative answer:
Name: google.com
Address: 142.250.196.78
Name: google.com
Address: 2404:6800:4007:82b::200e

[user@parrot]~]$ nslookup -q=WX google.com
*** Invalid option: q=WX
Server: 103.140.17.242
Address: 103.140.17.242#53

Non-authoritative answer:
Name: google.com
Address: 142.250.196.78
Name: google.com
Address: 2404:6800:4007:82b::200e
```

```
[user@parrot]~$ nslookup -q=WX google.com
*** Invalid option: q=WX
Server: 103.140.17.242
Address: 103.140.17.242#53

Non-authoritative answer:
Name: google.com
Address: 142.250.196.78

Name: google.com
Address: 2404:6800:4007:82b::200e

[user@parrot]~$ nslookup -type=SOA google.com
Server: 103.140.17.242
Address: 103.140.17.242#53

Non-authoritative answer:
google.com
origin = ns1.google.com
mail addr = dns-admin.google.com
serial = 396194125
refresh = 900
retry = 900
expire = 1800
minimum = 60

Authoritative answers can be found from:
```

```
[user@parrot]~$ nslookup -type=A google.com
Server: 103.140.17.242
Address: 103.140.17.242#53

Non-authoritative answer:
Name: google.com
Address: 142.250.196.78

[user@parrot]~$
```

Ifconfig

```
[user@parrot]~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.1.8 netmask 255.255.255.0 broadcast 192.168.1.255
          inet6 fe80::cf3a:cc49:d2fc:4813 prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:48:2c:b2 txqueuelen 1000 (Ethernet)
              RX packets 1451 bytes 116815 (114.0 KiB)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 739 bytes 63647 (62.1 KiB)
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
          inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
              RX packets 28 bytes 1568 (1.5 KiB)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 28 bytes 1568 (1.5 KiB)
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
[user@parrot]~$ ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.1.8 netmask 255.255.255.0 broadcast 192.168.1.255
          inet6 fe80::cf3a:cc49:d2fc:4813 prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:48:2c:b2 txqueuelen 1000 (Ethernet)
              RX packets 1465 bytes 117655 (114.8 KiB)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 739 bytes 63647 (62.1 KiB)
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
          inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
              RX packets 28 bytes 1568 (1.5 KiB)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 28 bytes 1568 (1.5 KiB)
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[user@parrot]~$ ifconfig -s
Iface      MTU     RX-OK RX-ERR RX-DRP RX-OVR     TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0      1500     1467      0      0 0        739       0       0       0 BMRU
lo       65536       28      0      0 0        28       0       0       0 LRU
```

```
[user@parrot]~$ ifconfig -v
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.8 netmask 255.255.255.0 broadcast 192.168.1.255
        inet6 fe80::cf3a:cc49:d2fc:4813 prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:48:2c:b2 txqueuelen 1000 (Ethernet)
                RX packets 1471 bytes 118015 (115.2 KiB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 739 bytes 63647 (62.1 KiB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
                RX packets 28 bytes 1568 (1.5 KiB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 28 bytes 1568 (1.5 KiB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[user@parrot]~$
```

LAMP INSTALLATION

Install apache

Update your system
sudo apt update

install Apache using apt:

sudo apt install apache2

Confirm that Apache is now running with the following command:

sudo systemctl status apache2

```
File Actions Edit View Help
└─(root㉿kali)-[~]
# systemctl start apache2

└─(root㉿kali)-[~]
# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: disabled)
   Active: active (running) since Sun 2021-10-03 05:42:27 EDT; 9s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 1357 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 1368 (apache2)
   Tasks: 6 (limit: 2296)
  Memory: 20.9M
    CPU: 163ms
   CGroup: /system.slice/apache2.service
           ├─1368 /usr/sbin/apache2 -k start
           ├─1370 /usr/sbin/apache2 -k start
           ├─1371 /usr/sbin/apache2 -k start
           ├─1372 /usr/sbin/apache2 -k start
           ├─1373 /usr/sbin/apache2 -k start
           └─1374 /usr/sbin/apache2 -k start

Oct 03 05:42:27 kali systemd[1]: Starting The Apache HTTP Server ...
Oct 03 05:42:27 kali apachectl[1367]: AH00558: apache2: Could not reliably determine the server's fully
Oct 03 05:42:27 kali systemd[1]: Started The Apache HTTP Server.
```



Apache2 Ubuntu Default Page

ubuntu

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

Install mariadb

- **Install mariaDB**

```
sudo apt install mariadb-server mariadb-client
```

- **Check mariadb Installation**

```
sudo systemctl status mysql
```

(if it is not working sudo systemctl start mysql)

```
[root@kali:~]# systemctl start mysql
[root@kali:~]# systemctl status mysql
● mariadb.service - MariaDB 10.5.12 database server
  Loaded: loaded (/lib/systemd/system/mariadb.service; disabled; vendor preset: disabled)
  Active: active (running) since Sun 2021-10-03 05:47:11 EDT; 9s ago
    Docs: man:mariadb(8)
          https://mariadb.com/kb/en/library/systemd/
   Process: 1415 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mysqld (code=exited, status=0/SUCCESS)
   Process: 1416 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)
   Process: 1418 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= || VAR=`cd /usr/bin/..; /usr/bin/galera_
   Process: 1481 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)
   Process: 1483 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
 Main PID: 1466 (mariadbd)
   Status: "Taking your SQL requests now..."
     Tasks: 15 (limit: 2296)
    Memory: 99.1M
      CPU: 389ms
     CGroup: /system.slice/mariadb.service
             └─1466 /usr/sbin/mariadbd

Oct 03 05:47:11 kali mariadb[1466]: 2021-10-03  5:47:11 3 [Warning] Access denied for user 'root'@'localhost' (using password)
Oct 03 05:47:11 kali mariadb[1466]: 2021-10-03  5:47:11 4 [Warning] Access denied for user 'root'@'localhost' (using password)
Oct 03 05:47:11 kali /etc/mysql/debian-start[1489]: Looking for 'mysql' as: /usr/bin/mysql
Oct 03 05:47:11 kali /etc/mysql/debian-start[1489]: Looking for 'mysqlcheck' as: /usr/bin/mysqlcheck
Oct 03 05:47:11 kali /etc/mysql/debian-start[1489]: Version check failed. Got the following error when calling the 'mysql' command
Oct 03 05:47:11 kali /etc/mysql/debian-start[1489]: ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password)
Oct 03 05:47:11 kali /etc/mysql/debian-start[1489]: FATAL ERROR: Upgrade failed
Oct 03 05:47:11 kali /etc/mysql/debian-start[1499]: Checking for insecure root accounts.
Oct 03 05:47:11 kali mariadb[1466]: 2021-10-03  5:47:11 5 [Warning] Access denied for user 'root'@'localhost' (using password)
Oct 03 05:47:11 kali debian-start[1502]: ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: NO)
[lines 1-28/28 (END)]
```

Install PHP

- **Install PHP**

```
sudo apt install php libapache2-mod-php php-ocache php-cli php-gd php-curl php-mysql
```

- **Restart apache2**

```
sudo systemctl restart apache2
```

- **Now you can check php installation**

```
sudo echo "<?php phpinfo(); ?>" | sudo tee -a  
/var/www/html/phpinfo.php >/dev/null
```

- **Open a browser**

<http://127.0.0.1/phpinfo.php>

PHP Version 7.4.3	
System	Linux kmabhijith-VirtualBox 5.11.0-27-generic #29~20.04.1-Ubuntu SMP Wed Aug 11 15:58:17 UTC 2021 x86_64
Build Date	Aug 13 2021 05:39:12
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.4/apache2
Loaded Configuration File	/etc/php/7.4/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.4/apache2/conf.d
Additional .ini files parsed	/etc/php/7.4/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.4/apache2/conf.d/10-opcache.ini, /etc/php/7.4/apache2/conf.d/10-pdo.ini, /etc/php/7.4/apache2/conf.d/15-xml.ini, /etc/php/7.4/apache2/conf.d/20-bz2.ini, /etc/php/7.4/apache2/conf.d/20-calendar.ini, /etc/php/7.4/apache2/conf.d/20-ctype.ini, /etc/php/7.4/apache2/conf.d/20-exif.ini, /etc/php/7.4/apache2/conf.d/20-fil.ini, /etc/php/7.4/apache2/conf.d/20-fileinfo.ini, /etc/php/7.4/apache2/conf.d/20-ftp.ini, /etc/php/7.4/apache2/conf.d/20-gd.ini, /etc/php/7.4/apache2/conf.d/20-gettext.ini, /etc/php/7.4/apache2/conf.d/20-iconv.ini, /etc/php/7.4/apache2/conf.d/20-isbn.ini, /etc/php/7.4/apache2/conf.d/20-mbstring.ini, /etc/php/7.4/apache2/conf.d/20-

Install phpmyadmin

```
sudo apt install phpmyadmin php-mbstring php-zip php-gd php-json php-curl  
( It ask for webserver select apache2, select db configuration and set password )
```

Restart apache2

```
sudo systemctl restart apache2
```

Check phpmyadmin

Open a browser

<http://localhost/phpmyadmin>

The image shows two screenshots of the phpMyAdmin interface.

The top screenshot shows the "Welcome to phpMyAdmin" page. It features a logo of a sailboat on water, a language selection dropdown set to "English", and a "Log in" form with "Username: root" and "Password: root" fields. A "Go" button is at the bottom right of the form.

The bottom screenshot shows the main database management interface. The left sidebar lists databases: New, information_schema, mysql, performance_schema, phpmyadmin, test, and user. The main area displays a table structure for the "user" table in the "test" database. The table has one row and one column named "Sum". The table details are as follows:

Table	Action	Rows	Type	Collation	Size	Overhead
user	Browse Structure Search Insert Empty Disp	1	InnoDB	utf8mb4_general_ci	16.7 KB	0 B
1 table	Sum		InnoDB	utf8mb4_general_ci	14.8 KB	0 B

Below the table, there are buttons for "Print", "Data dictionary", and "Create table". A "Name:" input field and a "Number of columns:" dropdown are also present.

Ansible Installation

Step1: sudo apt install ansible

```
[kali㉿kali)-[~]
$ sudo apt install ansible
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  ettercap-common ettercap-graphical libluajit-5.1-2 libluajit-5.1-common python3-qrcode
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  python3-argcomplete python3-httplib2 python3-jmespath python3-kerberos python3-libcloud python3-lockfile python3-selinux python3-winrm
Suggested packages:
  cowsay sshpass python-lockfile-doc
The following NEW packages will be installed:
  ansible python3-argcomplete python3-httplib2 python3-jmespath python3-kerberos python3-libcloud python3-lockfile python3-selinux python3-winrm
0 upgraded, 9 newly installed, 0 to remove and 815 not upgraded.
Need to get 19.6 MB of archives.
After this operation, 224 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://ftp.harukasan.org/kali kali-rolling/main amd64 python3-httplib2 all 0.18.1-3 [37.5 kB]
Get:2 http://ftp.harukasan.org/kali kali-rolling/main amd64 ansible all 2.10.7+merged+base+2.10.8+dfsg-1 [17.7 MB]
Get:3 http://ftp.harukasan.org/kali kali-rolling/main amd64 python3-argcomplete all 1.8.1-1.5 [29.7 kB]
Get:4 http://ftp.harukasan.org/kali kali-rolling/main amd64 python3-jmespath all 0.10.0-1 [21.7 kB]
Get:5 http://ftp.harukasan.org/kali kali-rolling/main amd64 python3-kerberos amd64 1.1.14-3.1+b3 [24.1 kB]
Get:6 http://ftp.harukasan.org/kali kali-rolling/main amd64 python3-lockfile all 1:0.12.2-2.2 [17.3 kB]
Get:7 http://ftp.harukasan.org/kali kali-rolling/main amd64 python3-libcloud all 3.2.0-2 [1,615 kB]
Get:8 http://ftp.harukasan.org/kali kali-rolling/main amd64 python3-selinux amd64 3.1-3 [160 kB]
Get:9 http://ftp.harukasan.org/kali kali-rolling/main amd64 python3-winrm all 0.4.1-0kaliz2 [32.1 kB]
Fetched 19.6 MB in 1min 15s (261 kB/s)
Selecting previously unselected package python3-httplib2.
(Reading database ... 275144 files and directories currently installed.)
Preparing to unpack .../0-python3-httplib2_0.18.1-3_all.deb ...
Unpacking python3-httplib2 (0.18.1-3) ...
Selecting previously unselected package ansible.
Preparing to unpack .../1-ansible_2.10.7+merged+base+2.10.8+dfsg-1_all.deb ...
Unpacking ansible (2.10.7+merged+base+2.10.8+dfsg-1) ...
Selecting previously unselected package python3-argcomplete.
Preparing to unpack .../2-python3-argcomplete_1.8.1-1.5_all.deb ...
Unpacking python3-argcomplete (1.8.1-1.5) ...
Selecting previously unselected package python3-jmespath.
Preparing to unpack .../3-python3-jmespath_0.10.0-1_all.deb ...
Unpacking python3-jmespath (0.10.0-1) ...
Selecting previously unselected package python3-kerberos.
Preparing to unpack .../4-python3-kerberos_1.1.14-3.1+b3_amd64.deb ...
Unpacking python3-kerberos (1.1.14-3.1+b3) ...
Selecting previously unselected package python3-lockfile.
Preparing to unpack .../5-python3-lockfile_1%3a0.12.2-2.2_all.deb ...
Unpacking python3-lockfile (1:0.12.2-2.2) ...
Selecting previously unselected package python3-libcloud.
Preparing to unpack .../6-python3-libcloud_3.2.0-2_all.deb ...
Unpacking python3-libcloud (3.2.0-2) ...
Selecting previously unselected package python3-selinux.
```

```

After this operation, 224 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://ftp.harukasan.org/kali kali-rolling/main amd64 python3-httplib2 all 0.18.1-3 [37.5 kB]
Get:2 http://ftp.harukasan.org/kali kali-rolling/main amd64 ansible all 2.10.7+merged+base+2.10.8+dfsg-1 [17.7 MB]
Get:3 http://ftp.harukasan.org/kali kali-rolling/main amd64 python3-argcomplete all 1.8.1-1.5 [29.7 kB]
Get:4 http://ftp.harukasan.org/kali kali-rolling/main amd64 python3-jmespath all 0.10.0-1 [21.7 kB]
Get:5 http://ftp.harukasan.org/kali kali-rolling/main amd64 python3-kerberos amd64 1.1.14-3.1+b3 [24.1 kB]
Get:6 http://ftp.harukasan.org/kali kali-rolling/main amd64 python3-lockfile all 1:0.12.2-2.2 [17.3 kB]
Get:7 http://ftp.harukasan.org/kali kali-rolling/main amd64 python3-libcloud all 3.2.0-2 [1,615 kB]
Get:8 http://ftp.harukasan.org/kali kali-rolling/main amd64 python3-selinux amd64 3.1-3 [160 kB]
Get:9 http://ftp.harukasan.org/kali kali-rolling/main amd64 python3-winrm all 0.4.1-0kali2 [32.1 kB]
Fetched 19.6 MB in 1min 15s (261 kB/s)
Selecting previously unselected package python3-httplib2.
(Reading database ... 275144 files and directories currently installed.)
Preparing to unpack .../0-python3-httplib2_0.18.1-3_all.deb ...
Unpacking python3-httplib2 (0.18.1-3) ...
Selecting previously unselected package ansible.
Preparing to unpack .../1-ansible_2.10.7+merged+base+2.10.8+dfsg-1_all.deb ...
Unpacking ansible (2.10.7+merged+base+2.10.8+dfsg-1) ...
Selecting previously unselected package python3-argcomplete.
Preparing to unpack .../2-python3-argcomplete_1.8.1-1.5_all.deb ...
Unpacking python3-argcomplete (1.8.1-1.5) ...
Selecting previously unselected package python3-jmespath.
Preparing to unpack .../3-python3-jmespath_0.10.0-1_all.deb ...
Unpacking python3-jmespath (0.10.0-1) ...
Selecting previously unselected package python3-kerberos.
Preparing to unpack .../4-python3-kerberos_1.1.14-3.1+b3_amd64.deb ...
Unpacking python3-kerberos (1.1.14-3.1+b3) ...
Selecting previously unselected package python3-lockfile.
Preparing to unpack .../5-python3-lockfile_1%3a0.12.2-2.2_all.deb ...
Unpacking python3-lockfile (1:0.12.2-2.2) ...
Selecting previously unselected package python3-libcloud.
Preparing to unpack .../6-python3-libcloud_3.2.0-2_all.deb ...
Unpacking python3-libcloud (3.2.0-2) ...
Selecting previously unselected package python3-selinux.
Preparing to unpack .../7-python3-selinux_3.1-3_amd64.deb ...
Unpacking python3-selinux (3.1-3) ...
Selecting previously unselected package python3-winrm.
Preparing to unpack .../8-python3-winrm_0.4.1-0kali2_all.deb ...
Unpacking python3-winrm (0.4.1-0kali2) ...
Setting up python3-lockfile (1:0.12.2-2.2) ...
Setting up python3-kerberos (1.1.14-3.1+b3) ...
Setting up python3-libcloud (3.2.0-2) ...
Setting up python3-jmespath (0.10.0-1) ...
Setting up python3-selinux (3.1-3) ...
Setting up python3-httplib2 (0.18.1-3) ...
Setting up python3-winrm (0.4.1-0kali2) ...
Setting up ansible (2.10.7+merged+base+2.10.8+dfsg-1) ...
Setting up python3-argcomplete (1.8.1-1.5) ...
Processing triggers for man-db (2.9.4-2) ...
Processing triggers for kali-menu (2021.2.3) ...

```

Installation check Step2:ansible –

version

```

[~] $ ansible --version
ansible 2.10.8
  config file = None
  configured module search path = ['/home/kali/.ansible/plugins/modules', '/usr/share/ansible/plugins/modules']
  ansible python module location = /usr/lib/python3/dist-packages/ansible
  executable location = /usr/bin/ansible
  python version = 3.9.2 (default, Feb 28 2021, 17:03:44) [GCC 10.2.1 20210110]

[~] $

```

Q. Execute **tcpdump** and its options on your own system, and submit the output screenshot as a document.

- **apt install tcpdump**

```
File Actions Edit View Help
└─(root💀kali㉿kali)-[~]
# apt install tcpdump
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  ettercap-common ettercap-graphical libluajit-5.1-2 libluajit-5.1-common python3-qrcode
Use 'apt autoremove' to remove them.
The following packages will be upgraded:
  tcpdump
1 upgraded, 0 newly installed, 0 to remove and 814 not upgraded.
Need to get 466 kB of archives.
After this operation, 1,024 B of additional disk space will be used.
Get:1 http://ftp.harukasan.org/kali kali-rolling/main amd64 tcpdump amd64 4.99.1-3 [466 kB]
Fetched 466 kB in 7s (62.8 kB/s)
(Reading database ... 312901 files and directories currently installed.)
Preparing to unpack .../tcpdump_4.99.1-3_amd64.deb ...
Unpacking tcpdump (4.99.1-3) over (4.99.0-2) ...
Setting up tcpdump (4.99.1-3) ...
Installing new version of config file /etc/apparmor.d/usr.bin.tcpdump ...
Processing triggers for man-db (2.9.4-2) ...
Processing triggers for kali-menu (2021.2.3) ...
```

- **tcpdump**

```
└─(root💀kali㉿kali)-[~]
# tcpdump
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
02:43:21.754837 ARP, Request who-has 192.168.192.217 (96:2d:01:da:8e:4a (oui Unknown)) tell 192.168.192.61, length 46
02:43:21.760206 ARP, Reply 192.168.192.217 is-at 96:2d:01:da:8e:4a (oui Unknown), length 46
02:43:21.849449 IP 192.168.192.254.41299 > 192.168.192.217.domain: 17304+ PTR? 217.192.168.192.in-addr.arpa. (46)
02:43:22.084082 IP 192.168.192.217.domain > 192.168.192.254.41299: 17304 NXDomain 0/0/0 (46)
02:43:22.084462 IP 192.168.192.254.59375 > 192.168.192.217.domain: 18006+ PTR? 61.192.168.192.in-addr.arpa. (45)
02:43:22.201501 IP 192.168.192.217.domain > 192.168.192.254.59375: 18006 NXDomain 0/0/0 (45)
02:43:22.201958 IP 192.168.192.254.56453 > 192.168.192.217.domain: 5023+ PTR? 254.192.168.192.in-addr.arpa. (46)
02:43:22.276058 IP 192.168.192.217.domain > 192.168.192.254.56453: 5023 NXDomain 0/0/0 (46)
02:43:25.752676 IP 192.168.192.61.59058 > sb-in-f188.1e100.net.https: Flags [.], seq 2091335895:2091335896, ack 4181321158, win 259, length 1
02:43:25.832062 IP 192.168.192.254.35986 > 192.168.192.217.domain: 21037+ PTR? 188.130.125.74.in-addr.arpa. (45)
02:43:26.172346 IP sb-in-f188.1e100.net.https > 192.168.192.61.59058: Flags [.], ack 1, win 265, options [nop,nop,sack 1 {0:1}], length 0
02:43:26.172348 IP 192.168.192.217.domain > 192.168.192.254.35986: 21037 1/0 PTR sb-in-f188.1e100.net. (79)
02:43:27.801975 ARP, Request who-has 192.168.192.217 tell 192.168.192.254, length 28
02:43:27.808941 ARP, Reply 192.168.192.217 is-at 96:2d:01:da:8e:4a (oui Unknown), length 46
02:43:29.074389 ARP, Request who-has 192.168.192.254 tell 192.168.192.217, length 46
02:43:29.074413 ARP, Reply 192.168.192.254 is-at 08:00:27:0e:34:8d (oui Unknown), length 28
02:43:30.921286 IP 192.168.192.61.49448 > 20.189.173.9.https: Flags [.], seq 165535, options [mss 1460,nop,wscale 8,nop,nop,sackOK], length 0
02:43:30.923227 IP 192.168.192.254.33085 > 192.168.192.217.domain: 44360+ PTR? 9.173.189.20.in-addr.arpa. (43)
02:43:31.187098 IP 192.168.192.217.domain > 192.168.192.254.33085: 44360 NXDomain 0/1/0 (129)
02:43:31.289465 IP 20.189.173.9.https > 192.168.192.61.49448: Flags [.], seq 4323786116, ack 3237987243, win 65535, options [mss 1360,nop,wscale 8,nop,nop,sackOK], length 0
02:43:31.289535 IP 192.168.192.61.49448 > 20.189.173.9.https: Flags [.], ack 1, win 1024, length 0
02:43:31.290040 IP 192.168.192.61.49448 > 20.189.173.9.https: Flags [.], seq 1:230, ack 1, win 1024, length 229
02:43:32.028761 IP 192.168.192.61.49448 > 20.189.173.9.https: Flags [.], seq 1:230, ack 1, win 1024, length 229
02:43:33.108010 IP 192.168.192.61.49448 > 20.189.173.9.https: Flags [.], seq 1:230, ack 1, win 1024, length 229
02:43:33.647058 IP 192.168.192.61.49448 > 20.189.173.9.https: Flags [.], ack 2721, win 1024, length 0
02:43:33.647063 IP 20.189.173.9.https > 192.168.192.61.49448: Flags [.], seq 1:2721, ack 230, win 2049, length 2720
02:43:33.648654 IP 20.189.173.9.https > 192.168.192.61.49448: Flags [.], seq 5441:6210, ack 230, win 2049, length 769
02:43:33.648656 IP 192.168.192.61.49448 > 20.189.173.9.https: Flags [.], ack 2721, win 1024, options [nop,nop,sack 1 {5441:6210}], length 0
02:43:33.648657 IP 20.189.173.9.https > 192.168.192.61.49448: Flags [.], seq 2721:4081, ack 230, win 2049, length 1360
02:43:33.648765 IP 192.168.192.61.49448 > 20.189.173.9.https: Flags [.], ack 4081, win 1024, options [nop,nop,sack 1 {5441:6210}], length 0
02:43:33.650175 IP 192.168.192.61.49448 > 20.189.173.9.https: Flags [.], ack 6210, win 1024, length 0
02:43:33.650177 IP 20.189.173.9.https > 192.168.192.61.49448: Flags [.], seq 4081:5441, ack 230, win 2049, length 1360
02:43:33.656752 IP 192.168.192.61.49448 > 20.189.173.9.https: Flags [.], seq 230:388, ack 6210, win 1024, length 158
02:43:33.922214 IP 20.189.173.9.https > 192.168.192.61.49448: Flags [.], seq 6719:6261, ack 388, win 2049, length 51
02:43:33.922216 IP 192.168.192.61.49448 > 20.189.173.9.https: Flags [.], ack 6261, win 1023, length 0
02:43:33.923291 IP 192.168.192.61.49448 > 20.189.173.9.https: Flags [.], seq 388:846, ack 6261, win 1023, length 458
02:43:34.257572 IP 20.189.173.9.https > 192.168.192.61.49448: Flags [.], seq 6261:6315, ack 846, win 2047, length 54
02:43:34.257574 IP 192.168.192.61.49448 > 20.189.173.9.https: Flags [.], seq 846:2206, ack 6315, win 1023, length 1360
02:43:34.596276 IP 20.189.173.9.https > 192.168.192.61.49448: Flags [.], ack 2206, win 2050, length 0
02:43:34.596279 IP 192.168.192.61.49448 > 20.189.173.9.https: Flags [.], seq 2206:3761, ack 6315, win 1023, length 1555
02:43:34.907308 IP 20.189.173.9.https > 192.168.192.61.49448: Flags [.], ack 3761, win 2050, length 0
02:43:34.907311 IP 20.189.173.9.https > 192.168.192.61.49448: Flags [.], seq 6319:6673, ack 3761, win 2050, length 358
02:43:34.907373 IP 192.168.192.61.49448 > 20.189.173.9.https: Flags [.], ack 6673, win 1022, length 0
02:44:11.161263 IP 192.168.192.61.59058 > sb-in-f188.1e100.net.https: Flags [.], seq 0:1, ack 1, win 259, length 1
02:44:11.419463 IP sb-in-f188.1e100.net.https > 192.168.192.61.59058: Flags [.], ack 1, win 265, options [nop,nop,sack 1 {0:1}], length 0
02:44:16.230215 IP 219.144.247.35.bc.googleusercontent.com.https > 192.168.192.61.60531: Flags [.], seq 2729959343:2729959374, ack 2617887749, win 160, length 31
02:44:16.231067 IP 192.168.192.61.60531 > 219.144.247.35.bc.googleusercontent.com.https: Flags [.], seq 1:32, ack 31, win 260, length 31
```

- `tcpdump -c 5`

SHELL SCRIPTING

1. Write a shell script to ask your name, and college name and print it on the screen.

```
#!/bin/bash
echo "enter your name";read you;
echo "enter college name"; read college;
clear
echo Details you entered
echo $you;
echo $college;
```

```
[(root💀kali)-[~/college/network]
# vi ques1.sh

[(root💀kali)-[~/college/network]
# bash ques1.sh
enter your name
NIMISHA JAMES
enter college name
Amal Jyothi College of Engineering]
```

```
Details you entered  
NIMISHA JAMES  
Amal Jyothi College of Engineering  
[root💀kali]-[~/college/network]  
#
```

1. Write a shell script to set a value for a variable and display it on command line interface.

```
#!/bin/bash  
((sum=10))  
echo "number is $sum"  
~  
~  
~  
~  
~  
~  
~  
~  
~  
~
```

```
[root💀kali]-[~/college/network]  
# bash ques2.sh  
number is 10  
[root💀kali]-[~/college/network]  
#
```

2. Write a shell script to perform addition, subtraction, multiplication, division with two numbers that is accepted from user.

```
#!/bin/bash
echo "enter two numbers";
read a b;
echo "addition $((a+b))";
echo "subtraction $((a-b))";
echo "division $((a/b))";
echo "multiplication $((a*b))";
~
```

```
[root@kali] ~[~/college/network]
# bash ques3.sh
enter two numbers
100 500
addition 600
subtraction -400
division 0
multiplication 50000
[root@kali] ~[~/college/network]
#
```

3. Write a shell script to check the value of a given number and display whether the number is found or not.

```
File Actions Edit View Help
#!/bin/bash
echo "enter a number"
read a
if [[ $a -eq 10 ]]
then
    echo "number found"
else
    echo "number not found"
fi
```

```
[root@kali] ~college/network]
# bash ques4.sh
enter a number
10
number found
```

4. Write a shell script to display current date, calendar

```
#!/bin/bash
echo "$(date)";
echo "calnder :";
cal
```

```
└─$ bash bash5.sh
Time and Calendar
_____
Today is Sat 02 Oct 2021 08:05:44 AM EDT
Calendar :
    October 2021
Su Mo Tu We Th Fr Sa
            1  2
3  4  5  6  7  8  9
10 11 12 13 14 15 16
17 18 19 20 21 22 23
24 25 26 27 28 29 30
31
```

5. Write a shell script to check a number is even or odd

```
#!/bin/bash
echo "enter a number";
read a;
if [[ $((a%2)) -eq 0 ]]
then
    echo "$a is even";
else
    echo "$a is odd";
fi
~
~
~
```

```
└─[root@kali]─[~/college/network]
# bash ques6.sh
enter a number
5
5 is odd
```

6. Write a shell script to check a number is greater than, less than or equal to another number.

```
#!/bin/bash
echo "enter a number";
read a;
if [[ $a -gt 10 ]]
then
    echo "number is grater than 10";
fi

if [[ $a -le 10 ]]
then
    echo "number is less than or equal to 10"
fi
~
```

```
[root@kali:~/college/network]
# bash ques7.sh
enter a number
100
number is grater than 10
```

7. Write a shell script to find the sum of first 10 numbers

```
#!/bin/bash
sum=0
n=10
echo "sum of first 10 numbers";
for ((i=1;i <= $n;i++ ))
do
    sum=$((sum+i))
done
echo "$sum";
```

```
[root@kali:~/college/network]
# bash ques8.sh
sum of first 10 numbers
55
```

8. Write a shell script to find the sum, the average and the product of the four integers entered.

```
#!/bin/bash
echo "enter four numbers";
read a b c d;
sum=$((a+b+c+d))
echo "sum is $sum";
avg=$((sum/4))
echo "average is $avg";
pro=$((a*b*c*d))
echo "product is $pro";
```

```
[root@kali:~/college/network]
# bash ques9.sh
enter four numbers
2 4 5 12
sum is 23
average is 5
product is 480
```

9. Write a shell script to find the smallest of three numbers.

```
File Actions Edit View Help
#!/bin/bash
echo "enter three numbers"
read a b c;
if [[ $a -lt $b ]]
then
    echo "$a is smaller";
elif [[ $b -lt $c ]]
then
    echo "$b is smaller";
else
    echo "$c is smaller";
fi
~
```

```
└─(root㉿kali)-[~/college/network]
# bash ques10.sh
enter three numbers
4 500 123
4 is smaller
```

10. Write a shell program to find factorial of given number.

```
#!/bin/bash
echo "enter a number";
read a;
fact=1;
while [ $a -ge 1 ]
do
fact=$((fact * $a))
a=$((a-1))
done
echo "factorial is $fact";
~
```

```
└─(root㉿kali)-[~/college/network]
# bash ques11.sh
enter a number
4
factorial is 24
```

11. Write a shell program to check a number is palindrome or not.

```
#!/bin/bash
echo "enter a number";
read a;
pali=$a;
num=0;
while [ $a -gt 0 ]
do
    digit=$((a%10));
    num=$((num*10))+$digit;
    a=$((a/10));

done
if [[ $num -eq $pali ]]
then
    echo "$pali is palindrome";
else
    echo "$pali is not palindrome";
fi
~
```

```
[root@kali] ~college/network]
# bash ques12.sh
enter a number
6
6 is palindrome
```

12. Write a shell script to find the average of the numbers entered in command line.

```
#!/bin/bash
echo "enter number of numbers";
read n;
sum=0;
echo "enter numbers";
for((i=0;i<n;i++))
do
    read a;
    sum=$((sum + a));
done
avg=$((sum/n));
echo "average is $avg"
~
```

```
[root@kali ~]# bash ques13.sh
enter number of numbers
2
enter numbers
5
77
average is 41
```

13. Write a shell program to find the sum of all the digits in a number.

```
#!/bin/bash
echo "enter a number";
read a;
pali=$a;
num=0;
while [ $a -gt 0 ]
do
    digit=$((a%10));
    num=$((digit+num));
    a=$((a/10));
done
echo "sum of digits of $pali is $num";
```

```
[root@kali ~]# bash ques14.sh
enter a number
167
sum of digits of 167 is 14
```

14. Write a shell Script to check whether given year is leap year or not.

```
File Actions Edit View Help
#!/bin/bash
echo "enter the year";
read a;
year=$((a%4));
if [[ $year -eq 0 ]]
then
    echo "$a is leap year";
else
    echo "$a is a normal year";
fi
~
```

```
└─(root㉿kali)-[~/college/network]
└─# bash ques15.sh
enter the year
2020
2020 is leap year

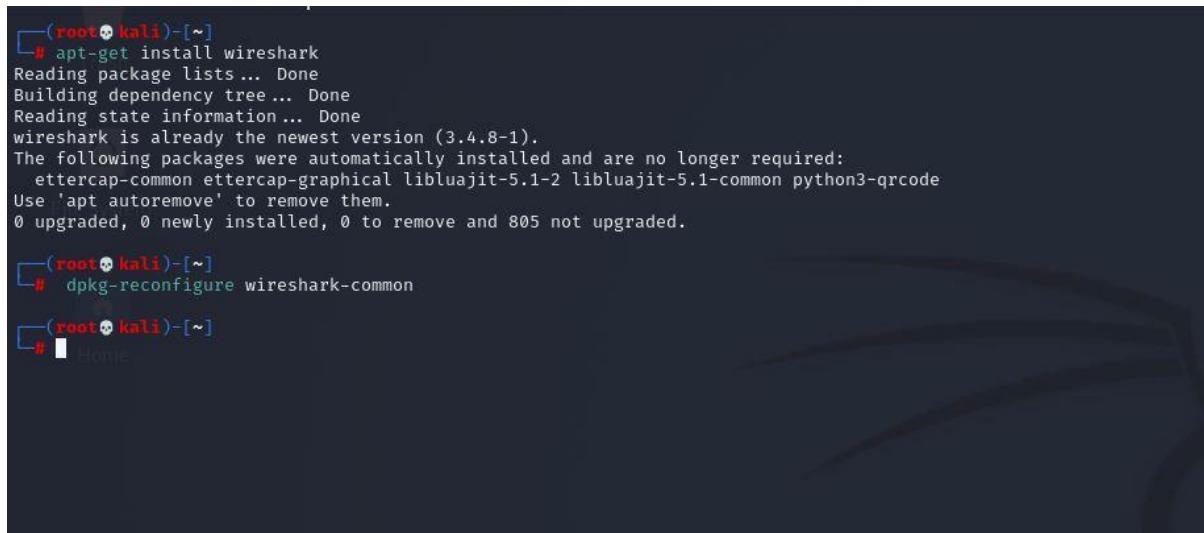
└─(root㉿kali)-[~/college/network]
└─# bash ques15.sh
enter the year
2022
2022 is a normal year

└─(root㉿kali)-[~/college/network]
└─#
```

Analyzing network packet stream using nc and wireshark

Step1:

- `sudo apt-get install wireshark`



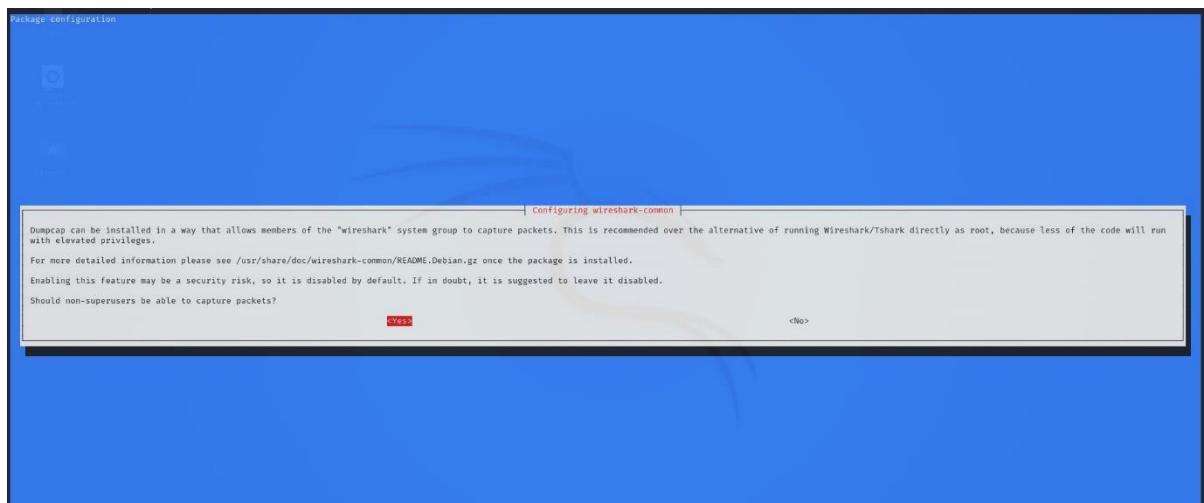
```
(root㉿kali)-[~]
# apt-get install wireshark
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
wireshark is already the newest version (3.4.8-1).
The following packages were automatically installed and are no longer required:
  ettercap-common ettercap-graphical libluajit-5.1-2 libluajit-5.1-common python3-qrcode
Use 'apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 805 not upgraded.

(root㉿kali)-[~]
# dpkg-reconfigure wireshark-common

(root㉿kali)-[~]
#
```

Step2:

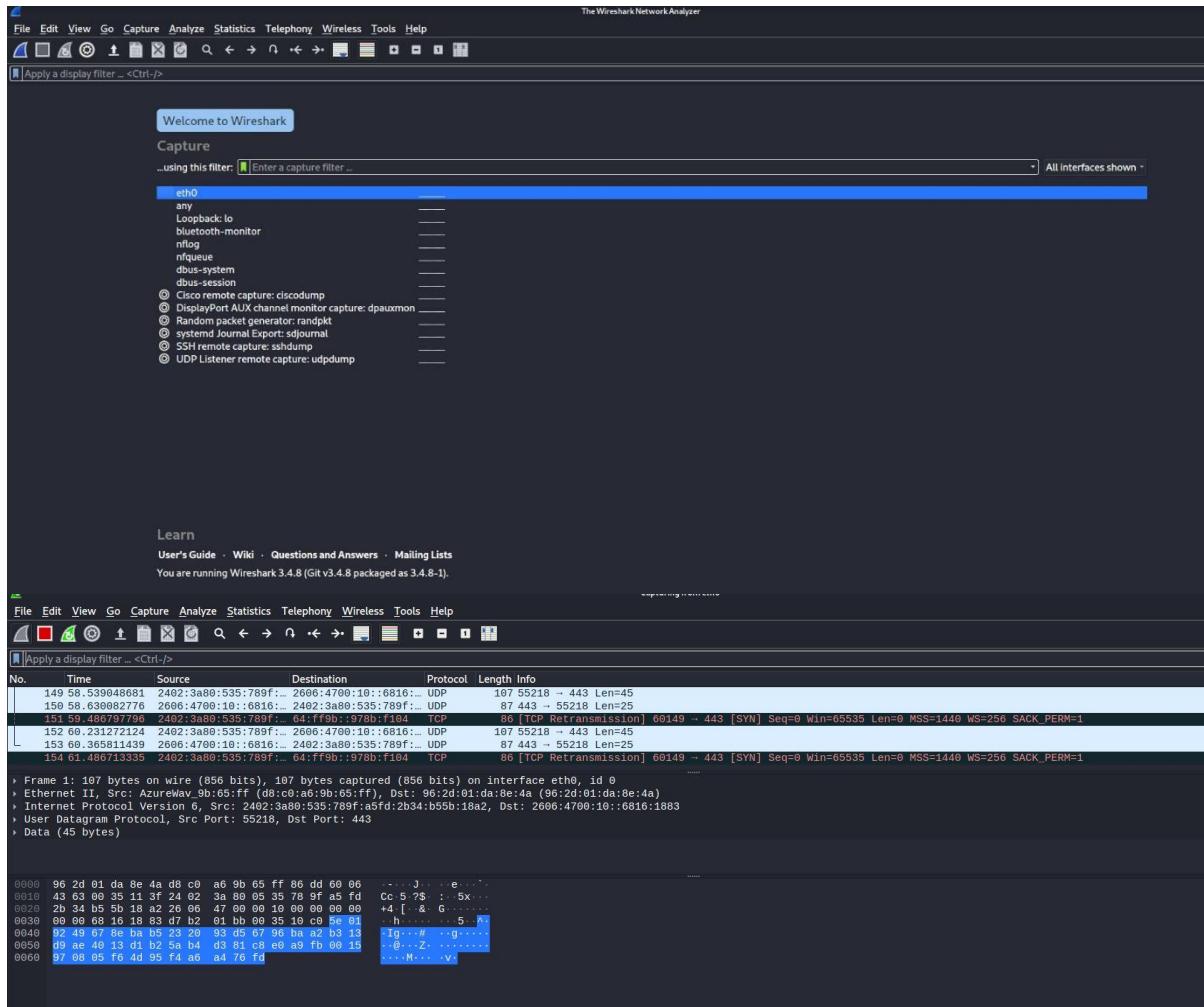
- `sudo dpkg-reconfigure wireshark-common`



Step3.

open wireshark from the applist

20MCA136 - Networking & System Administration Lab



DOCKER INSTALLATION

Step1

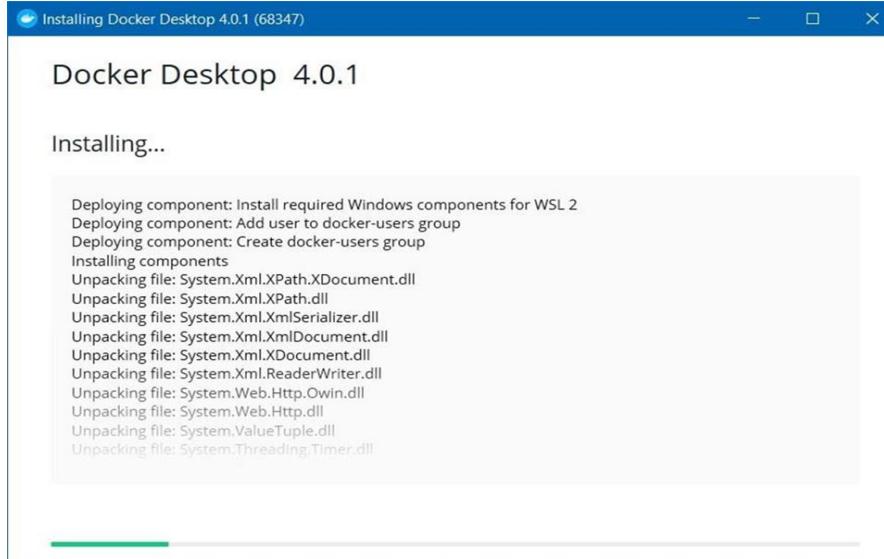
Download Docker desktop Installer for Windows from

<https://desktop.docker.com/win/main/amd64/Docker%20Desktop%20Installer.exe>



Step-II

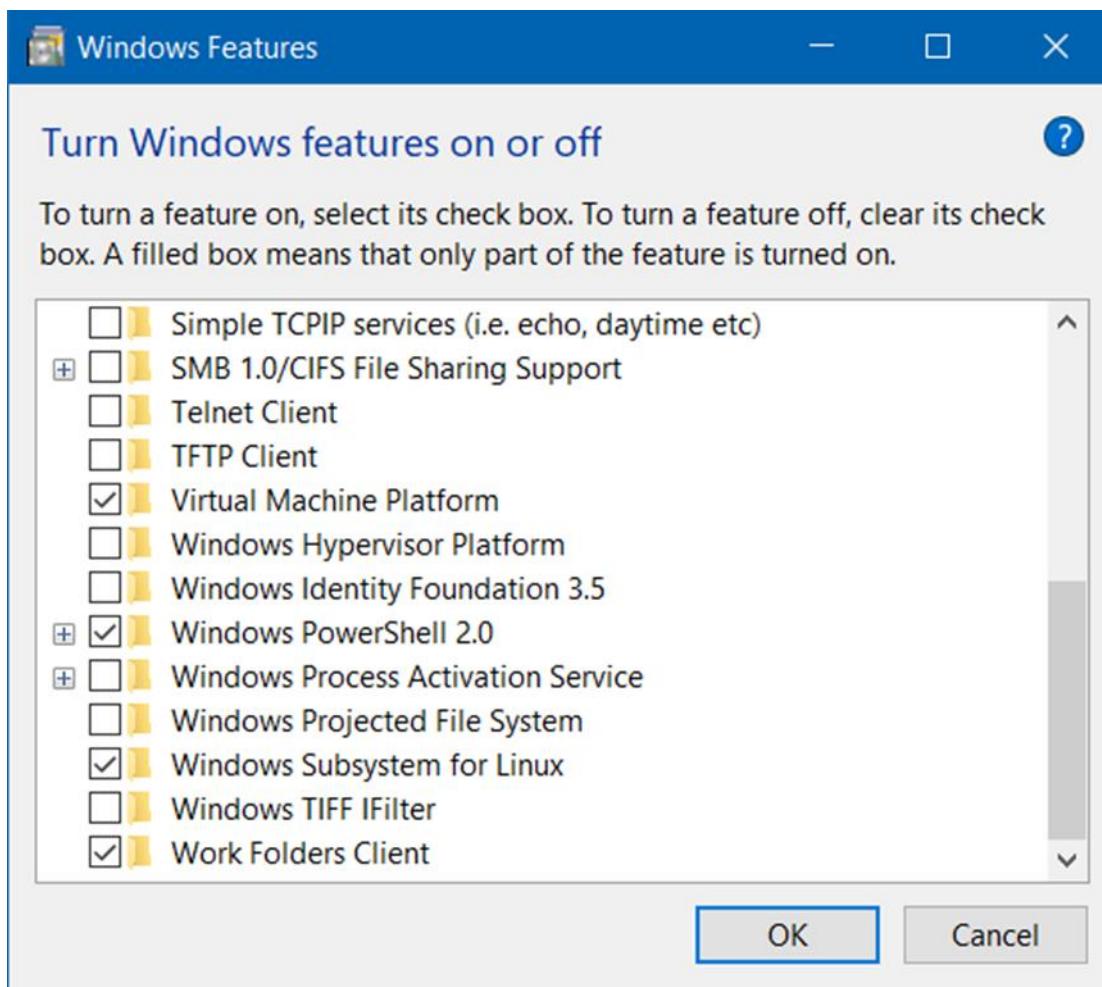
Open the .exe file and follow the steps after clicking install button.



Step-III

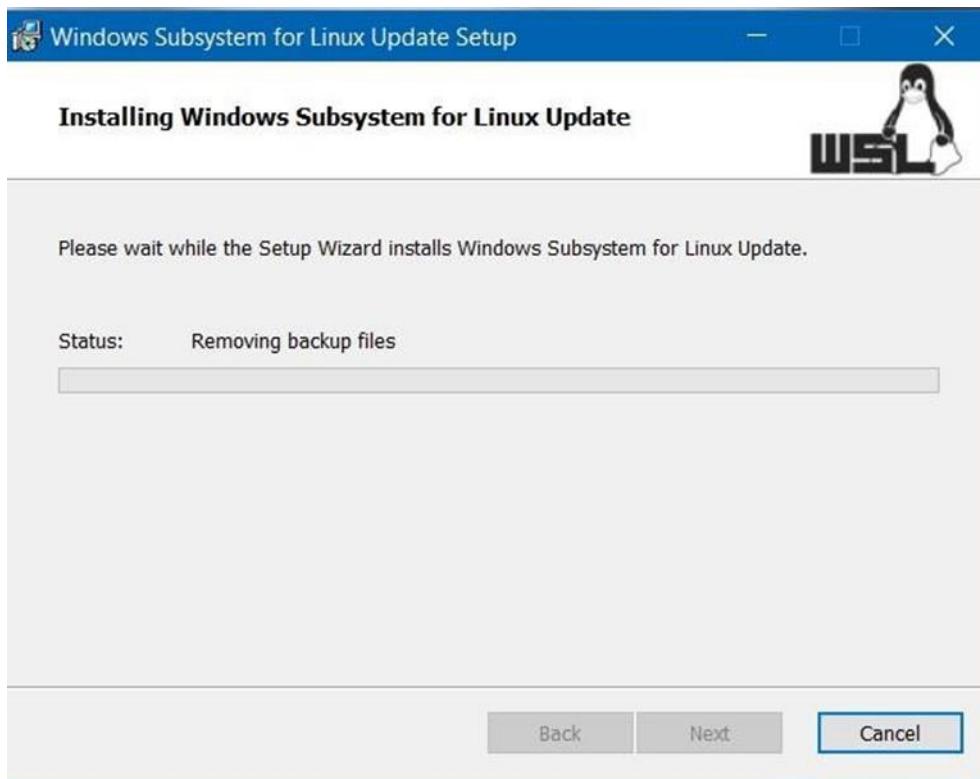
Once installed go to programs and features and click turn on windows features on or off

Scroll to the bottom and select windows subsystem for Linux.



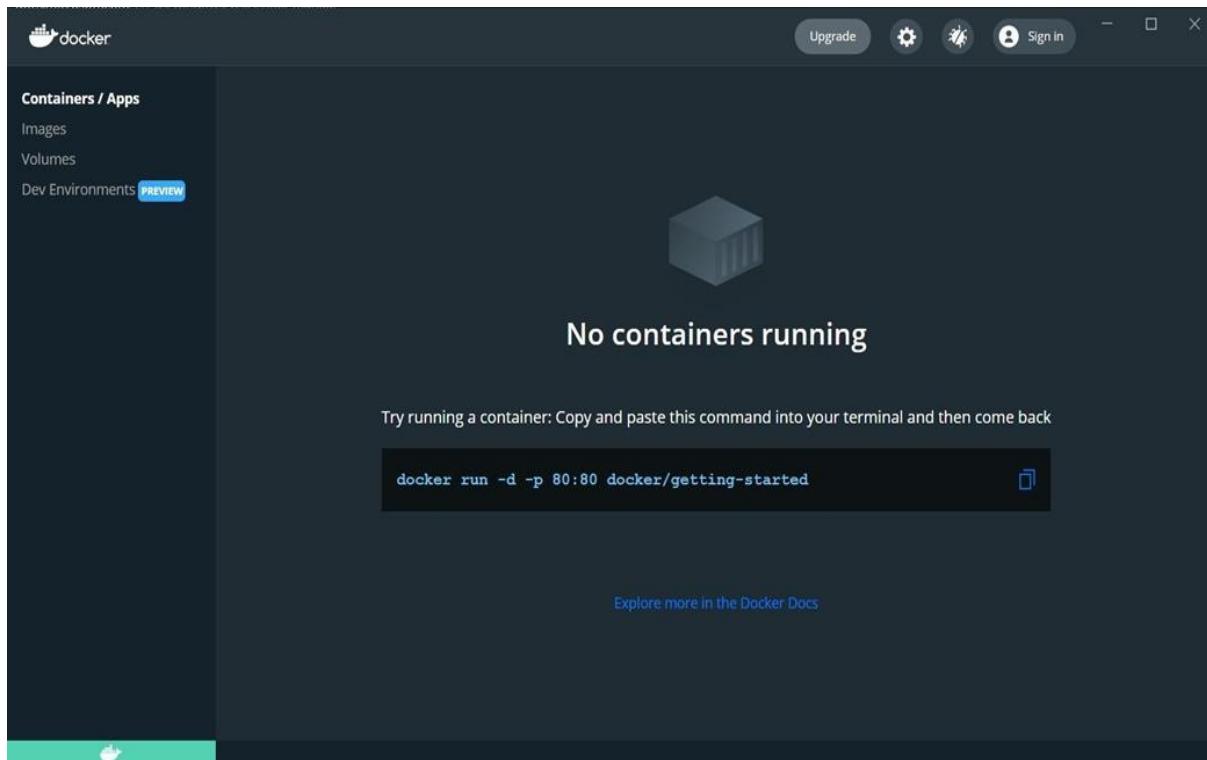
Step-IV

If any WSL 2 error occurs download windows subsystem for linux update package and install the .exe file, after the installation restart the windows device.



Step-V

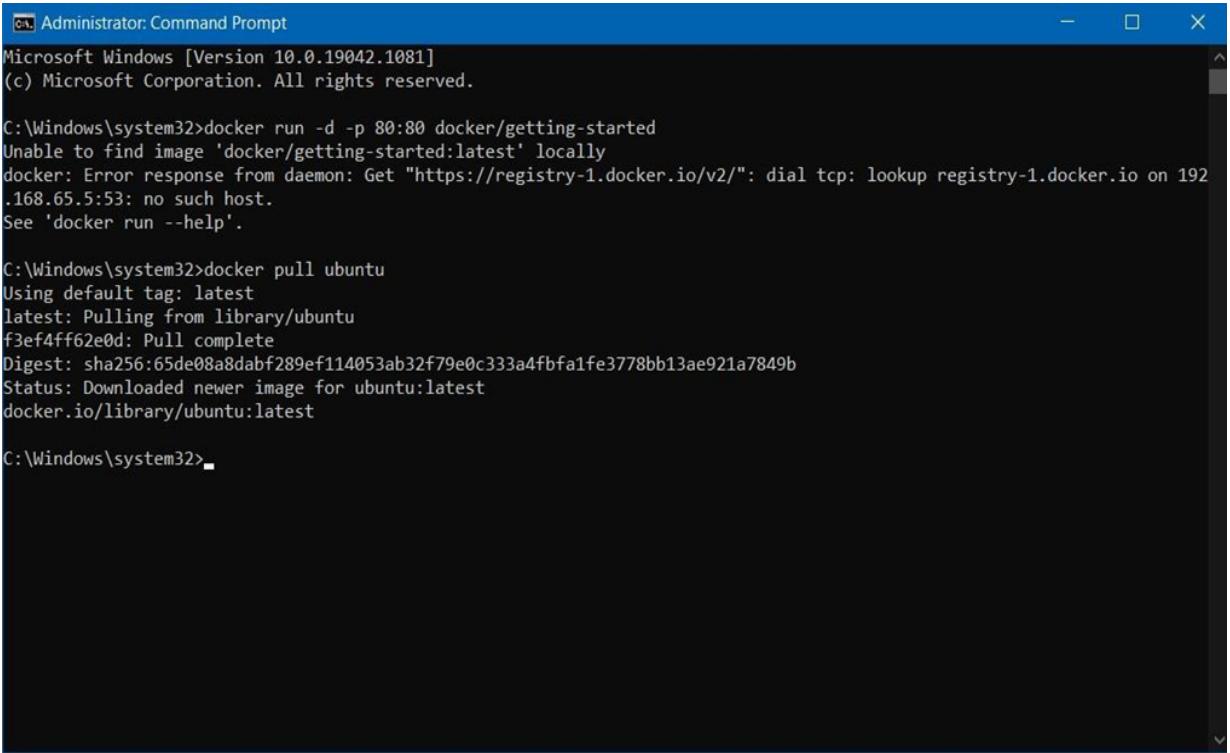
Once installed, open the docker desktop app, and signin using the dockerID



Step-VI

Now pull any image from docker hub using the docker pull command in the command prompt (eg: docker pull ubuntu).

20MCA136 - Networking & System Administration Lab



The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". The title bar includes standard window controls (minimize, maximize, close) and a vertical scroll bar on the right. The command line shows the following sequence of Docker commands:

```
C:\Windows\system32>docker run -d -p 80:80 docker/getting-started
Unable to find image 'docker/getting-started:latest' locally
docker: Error response from daemon: Get "https://registry-1.docker.io/v2/": dial tcp: lookup registry-1.docker.io on 192.168.65.5:53: no such host.
See 'docker run --help'.

C:\Windows\system32>docker pull ubuntu
Using default tag: latest
latest: Pulling from library/ubuntu
f3ef4ff62e0d: Pull complete
Digest: sha256:65de08a8dabf289ef114053ab32f79e0c333a4fbfa1fe3778bb13ae921a7849b
Status: Downloaded newer image for ubuntu:latest
docker.io/library/ubuntu:latest

C:\Windows\system32>
```

Now in the images tab an image of ubuntu will be displayed, we can run the ubuntu instance using the cli.

20MCA136 - Networking & System Administration Lab

