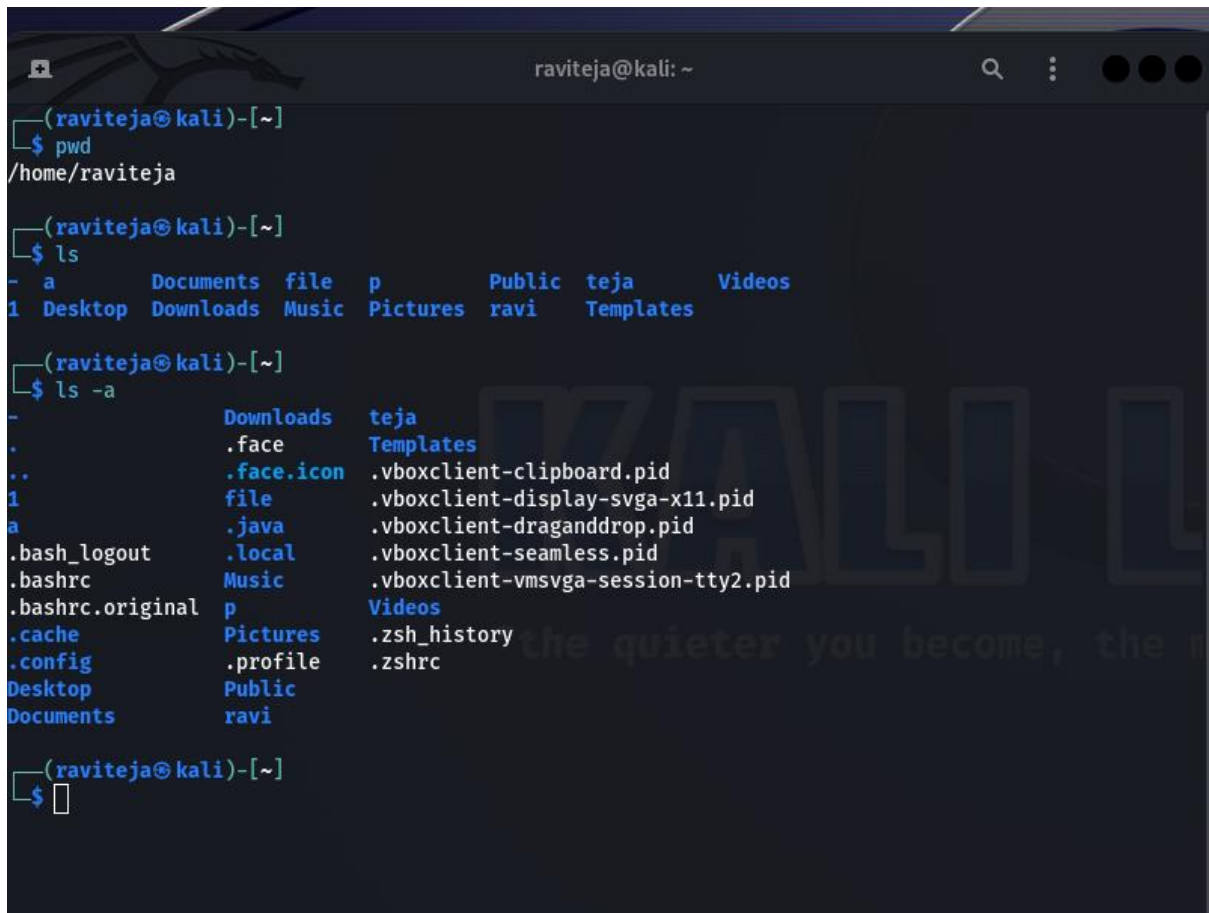


1.

- (a.) Display the path of your current directory
- (b.) List out the contents of your current directory
- (c.) List out the contents of your current directory including hidden files



```
(raviteja@kali)-[~]
└─$ pwd
/home/raviteja

(raviteja@kali)-[~]
└─$ ls
- a      Documents  file  p      Public  teja      Videos
1 Desktop  Downloads Music  Pictures ravi     Templates

(raviteja@kali)-[~]
└─$ ls -a
-      Downloads  teja
.      .face       Templates
..     .face.icon  .vboxclient-clipboard.pid
1      file      .vboxclient-display-svg-x11.pid
a      .java      .vboxclient-draganddrop.pid
.bash_logout .local     .vboxclient-seamless.pid
.bashrc      Music      .vboxclient-vmsvga-session-tty2.pid
.bashrc.original p          Videos
.cache       Pictures   .zsh_history
.config      .profile  .zshrc
Desktop      Public
Documents    ravi
```

2.

- (a.) Create a new directory named a
- (b.) Move to the newly created directory a
- (c.) Create a blank file named “file1”
- (d.) Display the file type of “file1”
- (e.) Add the line “Hello World” to “file1” using the command
- (f.) Display the contents of “file1”
- (g.) Display the file type of “file1” again

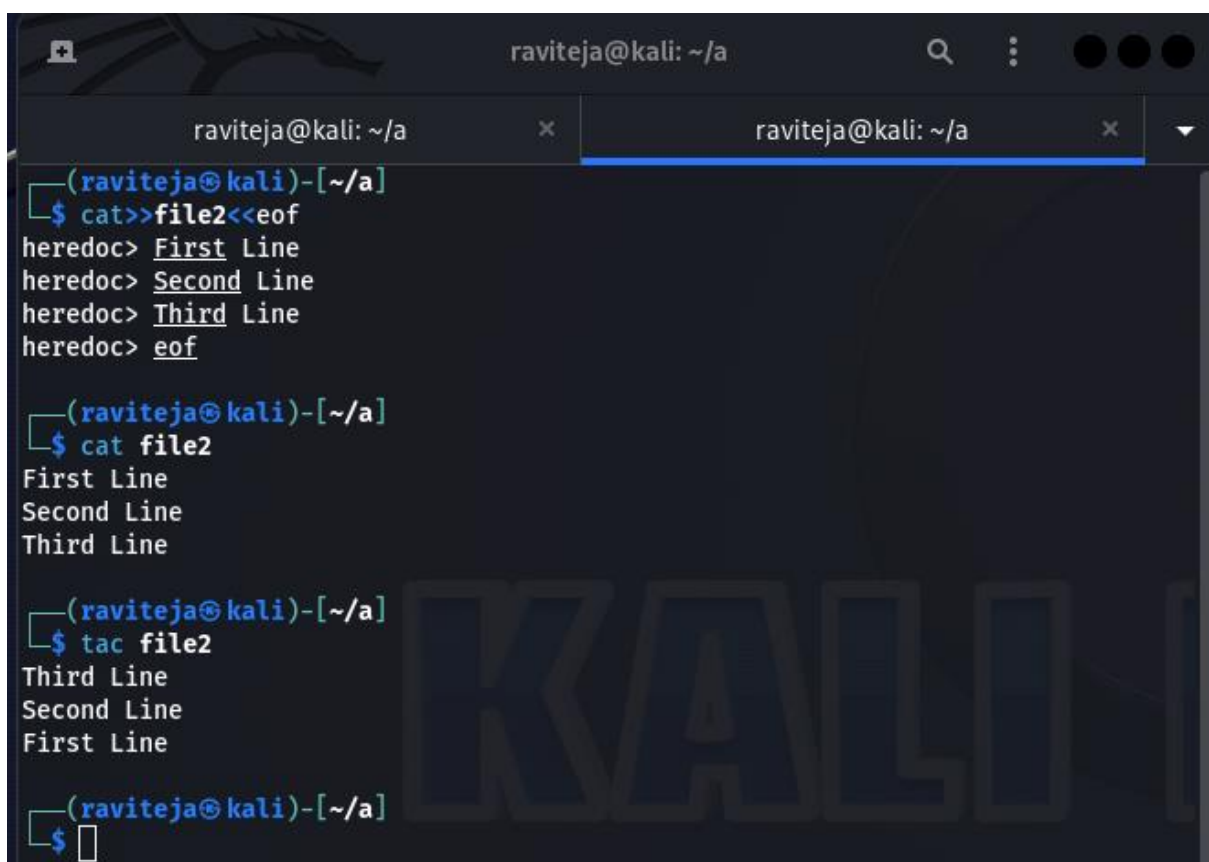
3.

(a.) Stay in directory a. Create a file “file2” and add the contents below using the `cat` command

First Line Second Line Third Line

(b.) Display the contents of “file2”

(c.) Display the contents of “file2” with the lines reversed

A terminal window titled 'raviteja@kali: ~/a' with two tabs. The first tab shows the creation of 'file2' using a heredoc with three lines: 'First Line', 'Second Line', and 'Third Line'. The second tab shows the contents of 'file2' using 'cat', displaying the same three lines. The third tab shows the contents of 'file2' using 'tac', displaying the lines in reverse order: 'Third Line', 'Second Line', and 'First Line'.

```
(raviteja@kali)-[~/a]
└─$ cat >>file2<<eof
heredoc> First Line
heredoc> Second Line
heredoc> Third Line
heredoc> eof

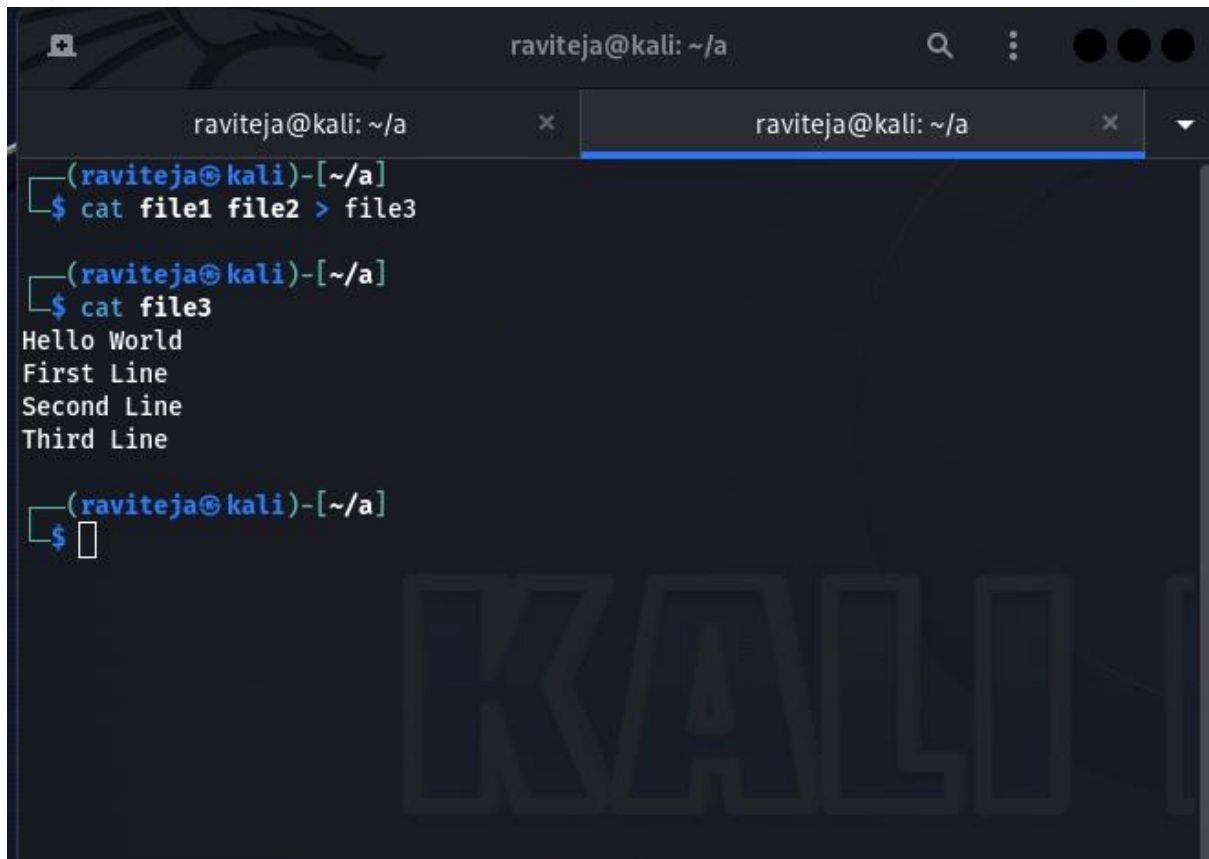
(raviteja@kali)-[~/a]
└─$ cat file2
First Line
Second Line
Third Line

(raviteja@kali)-[~/a]
└─$ tac file2
Third Line
Second Line
First Line

(raviteja@kali)-[~/a]
└─$
```

4.

- (a.) Stay in directory a. Concatenate the contents of “file1” and “file2” and save them into a new file “file3”
- (b.) Display the contents of “file3”



```
raviteja@kali: ~/a
(raviteja@kali)-[~/a]
$ cat file1 file2 > file3

(raviteja@kali)-[~/a]
$ cat file3
Hello World
First Line
Second Line
Third Line

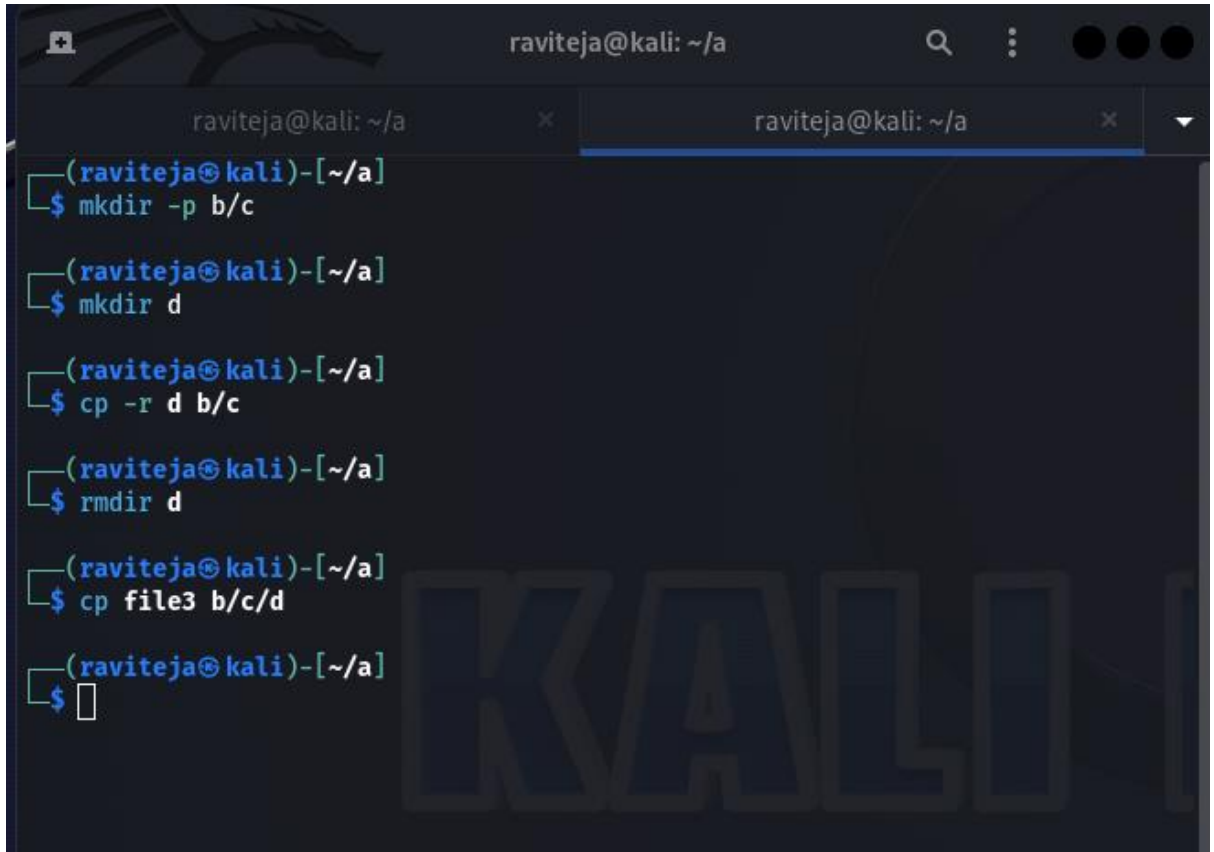
(raviteja@kali)-[~/a]
$
```

The image shows a terminal window with two tabs, both titled 'raviteja@kali: ~/a'. The active tab displays a series of commands and their outputs. First, the command 'cat file1 file2 > file3' is executed. Then, the command 'cat file3' is executed, resulting in the output: 'Hello World', 'First Line', 'Second Line', and 'Third Line'. The prompt '\$' is shown at the end of the last line, indicating the terminal is ready for the next command.

5.

- (a.) Stay in directory a. Create 2 directories b/c with a single command
- (b.) Create a new directory d
- (c.) Copy the directory d to directory c using a single command
- (d.) Delete the directory d in the current directory a

- (e.) Copy “file3” to the directory d with a single command

A terminal window titled 'raviteja@kali: ~/a' with two tabs. The terminal shows a series of commands and their outputs. The commands are: 'mkdir -p b/c', 'mkdir d', 'cp -r d b/c', 'rmdir d', 'cp file3 b/c/d', and a final prompt '\$ ' with a cursor. The background has a faint 'KALI' watermark.

```
(raviteja@kali)-[~/a]
$ mkdir -p b/c

(raviteja@kali)-[~/a]
$ mkdir d

(raviteja@kali)-[~/a]
$ cp -r d b/c

(raviteja@kali)-[~/a]
$ rmdir d

(raviteja@kali)-[~/a]
$ cp file3 b/c/d

(raviteja@kali)-[~/a]
$ 
```

6.

- (a.) Go to directory d and rename “file3” to “file0”
- (b.) Stay in the same directory and move “file0” to directory a

```
(raviteja@kali)-[~/a]
$ mv file3 file0

(raviteja@kali)-[~/a]
$ cd

(raviteja@kali)-[~]
$ mv a/b/c/d/file0 a
```

7.

- (a.) Go to your home directory
- (b.) Create a file named “test” in the directory a/b/c/d
- (c.) Stay in the home directory. Find and display the path of “test”

```
raviteja@kali: ~/a/b
(raviteja@kali)-[~]
$ cd

(raviteja@kali)-[~]
$ cd a/b/c/d

(raviteja@kali)-[~/a/b/c/d]
$ touch test

(raviteja@kali)-[~/a/b/c/d]
$ cat a/b/c/d/test
```

8.

- (a.) Go to directory a. Get the man page of grep and save its contents to a file named “grepman.txt”
- (b.) Print the lines containing the word “FILE” (Case sensitive) in the file “grepman.txt”

```
(raviteja@kali)-[~]
$ cd a

(raviteja@kali)-[~/a]
$ man grep > grepman.txt

(raviteja@kali)-[~/a]
$
```

```
(raviteja@kali)-[~/a]  
$ man grep | tee grepman.txt
```

GREP(1)

User Commands

GREP(1)

NAME

grep, egrep, fgrep, rgrep - print lines that match patterns

SYNOPSIS

```
grep [OPTION...] PATTERNS [FILE...]  
grep [OPTION...] -e PATTERNS ... [FILE...]  
grep [OPTION...] -f PATTERN_FILE ... [FILE...]
```

DESCRIPTION

grep searches for PATTERNS in each FILE. PATTERNS is one or more patterns separated by newline characters, and grep prints each line that matches a pattern. Typically PATTERNS should be quoted when grep is used in a shell command.

A FILE of "-" stands for standard input. If no FILE is given, recursive searches examine the working directory, and nonrecursive searches read standard input.

Debian also includes the variant programs egrep, fgrep and rgrep. These programs are the same as grep -E, grep -F, and grep -r, respectively. These variants are deprecated upstream, but Debian provides for backward compatibility. For portability reasons, it is recommended to avoid the variant programs, and use grep with the related option instead.

OPTIONS

Generic Program Information

--help Output a usage message and exit.

-V, --version

Output the version number of grep and exit.

Pattern Syntax

-E, --extended-regexp

Interpret PATTERNS as extended regular expressions (EREs, see below).

-F, --fixed-strings

Interpret PATTERNS as fixed strings, not regular expressions.

-G, --basic-regexp

Interpret PATTERNS as basic regular expressions (BREs, see below). This is the default.

9.

- (a.) Go to directory a and remove the directory b with a single command
- (b.) Remove the files starting with the word “file” with a single command

```
raviteja@kali: ~/a  
  
(raviteja@kali)-[~]  
$ cd a  
  
(raviteja@kali)-[~/a]  
$ rm b/c/d/test  
  
(raviteja@kali)-[~/a]  
$ rmdir -p b/c/d
```

B

```
(raviteja@kali)-[~/a]  
$ mv file3 file0  
  
(raviteja@kali)-[~/a]  
$ cd  
  
(raviteja@kali)-[~]  
$ mv a file0
```

10.

(a.) Download the compressed file from the drive.

<https://drive.google.com/drive/folders/1PG3ZlpFu6nQSNjpCNuceoGcNeY00bhPP?usp=sharing>

(b.) Extract the compressed file using CLI.

(c.) Decode the base64 content and display the content of “Flag.txt”using CLI.

```
raviteja@kali: ~/Downloads/BIOS (1)/Bash-Bi0s Pentest/Fi...
(raviteja@kali)-[~/Downloads/BIOS (1)/Bash-Bi0s Pentest]
$ tar -xvf Filez.tar.gz
Filez/
Filez/Flag.txt

(raviteja@kali)-[~/Downloads/BIOS (1)/Bash-Bi0s Pentest]
$ cd Filez

(raviteja@kali)-[~/Downloads/BIOS (1)/Bash-Bi0s Pentest/Filez]
$ base64 -d Flag.txt
You Found The Flag.

(raviteja@kali)-[~/Downloads/BIOS (1)/Bash-Bi0s Pentest/Filez]
$ cat Flag.txt
WW91IEZvdW5kIFRoZSBGbGFnLg==

(raviteja@kali)-[~/Downloads/BIOS (1)/Bash-Bi0s Pentest/Filez]
$
```

11.

- (a.) Go to <https://blog.bi0s.in/> and download the logo.png image using wget
- (b.) Do the same using curl

```
(raviteja@kali)-[~/z]
└─$ curl -O https://blog.bi0s.in/assets/logo.png
  % Total    % Received % Xferd  Average Speed   Time    Time     Current
                                 Dload  Upload   Total   Spent    Left     Speed
100 22693  100 22693    0     0  17797      0  0:00:01  0:00:01 --:--:-- 17840

(raviteja@kali)-[~/z]
└─$ curl -O
curl: no URL specified!
curl: try 'curl --help' or 'curl --manual' for more information

(raviteja@kali)-[~/z]
└─$ curl -O pic.png https://blog.bi0s.in/assets/logo.png
  % Total    % Received % Xferd  Average Speed   Time    Time     Current
                                 Dload  Upload   Total   Spent    Left     Speed
100 22693  100 22693    0     0  20499      0  0:00:01  0:00:01 --:--:-- 20592

(raviteja@kali)-[~/z]
└─$ ls
logo.png  pic.png

(raviteja@kali)-[~/z]
└─$ wget https://blog.bi0s.in/assets/logo.png
--2023-03-21 12:45:27-- https://blog.bi0s.in/assets/logo.png
Resolving blog.bi0s.in (blog.bi0s.in)... 104.21.14.171, 172.67.160.22, 2606:4700:3033::ac43:a016, ...
Connecting to blog.bi0s.in (blog.bi0s.in)|104.21.14.171|:443... connected.
HTTP request sent, awaiting response... 200 OK
length: 22693 (22K) [image/png]
Saving to: 'logo.png.1'

logo.png.1
100%[=====]
2023-03-21 12:45:28 (1.96 MB/s) - 'logo.png.1' saved [22693/22693]

(raviteja@kali)-[~/z]
└─$ ls
logo.png  logo.png.1  pic.png
```

12.

(a.) Ping google.com and find the lowest time taken to get a response
(Stop pinging after getting 5 responses)

Ans The lowest time taken to get a response is 49.3 ms third time

(b.) Ping google.com 6 times and find the average time taken to get a response

Ans Average time taken to get a response is 53.561 ms

```
(raviteja@kali)-[~/z]
$ ping -w 5 www.google.com
PING www.google.com (172.217.174.68) 56(84) bytes of data.
64 bytes from bom07s25-in-f4.1e100.net (172.217.174.68): icmp_seq=1 ttl=118 time=60.3 ms
64 bytes from bom07s25-in-f4.1e100.net (172.217.174.68): icmp_seq=2 ttl=118 time=50.9 ms
64 bytes from bom07s25-in-f4.1e100.net (172.217.174.68): icmp_seq=3 ttl=118 time=49.3 ms
64 bytes from bom07s25-in-f4.1e100.net (172.217.174.68): icmp_seq=4 ttl=118 time=49.8 ms
64 bytes from bom07s25-in-f4.1e100.net (172.217.174.68): icmp_seq=5 ttl=118 time=62.2 ms

--- www.google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4021ms
rtt min/avg/max/mdev = 49.334/54.499/62.165/5.543 ms

(raviteja@kali)-[~/z]
$ ping -c 6 google.com
PING google.com (142.250.77.46) 56(84) bytes of data.
64 bytes from bom07s26-in-f14.1e100.net (142.250.77.46): icmp_seq=1 ttl=118 time=50.5 ms
64 bytes from bom07s26-in-f14.1e100.net (142.250.77.46): icmp_seq=2 ttl=118 time=62.2 ms
64 bytes from bom07s26-in-f14.1e100.net (142.250.77.46): icmp_seq=3 ttl=118 time=49.5 ms
64 bytes from bom07s26-in-f14.1e100.net (142.250.77.46): icmp_seq=4 ttl=118 time=50.2 ms
64 bytes from bom07s26-in-f14.1e100.net (142.250.77.46): icmp_seq=5 ttl=118 time=50.7 ms
64 bytes from bom07s26-in-f14.1e100.net (142.250.77.46): icmp_seq=6 ttl=118 time=58.3 ms

--- google.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5043ms
rtt min/avg/max/mdev = 49.473/53.561/62.184/4.876 ms

(raviteja@kali)-[~/z]
$
```

13.

Connect to your own system using telnet

```

--(raviteja@kali)-[~]
$ sudo apt install telnet
[sudo] password for raviteja:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  inetutils-telnetd
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
  telnet
0 upgraded, 1 newly installed, 0 to remove and 417 not upgraded.
Need to get 41.0 kB of archives.
After this operation, 54.3 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 telnet all 0.17+2.4-2 [41.0 kB]
Fetched 41.0 kB in 1s (36.5 kB/s)
Selecting previously unselected package telnet.
(Reading database ... 498540 files and directories currently installed.)
Preparing to unpack .../telnet_0.17+2.4-2_all.deb ...
Unpacking telnet (0.17+2.4-2) ...
Setting up telnet (0.17+2.4-2) ...

--(raviteja@kali)-[~]
$ ufw allow 23/tcp
ERROR: You need to be root to run this script

--(raviteja@kali)-[~]
$ sudo ufw allow 23/tcp
Skipping adding existing rule
Skipping adding existing rule (v6)

--(raviteja@kali)-[~]
$ sudo ufw reload
Firewall reloaded

--(raviteja@kali)-[~]
$ telnet localhost 23

```

14.

- (a.) Learn about nmap and use that scanner to scan your own machine
- (b.) Use nmap to scan scanme.nmap.org

```

--(raviteja@kali)-[~/z]
$ nmap -F 10.0.2.15
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-21 13:22 EDT
Nmap scan report for 10.0.2.15
Host is up (0.000052s latency).
All 100 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 100 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds

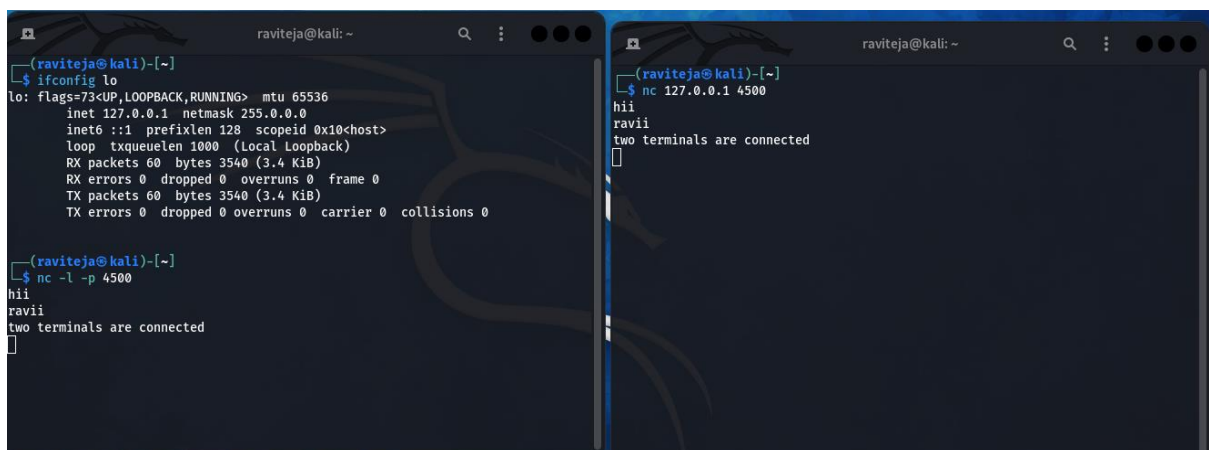
--(raviteja@kali)-[~/z]
$ nmap scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-21 13:23 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.30s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 69.22 seconds

```

15.

(a.) Create a chat application using nc on your local machine with one terminal as server and other as the client



```
(raviteja@kali)-[~]
$ ifconfig lo
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 60 bytes 3540 (3.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 60 bytes 3540 (3.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(raviteja@kali)-[~]
$ nc -l -p 4500
hii
ravii
two terminals are connected

(raviteja@kali)-[~]
$ nc 127.0.0.1 4500
hii
ravii
two terminals are connected
```

(b.) Transfer a file from server to client (save that file with another name) and display the file.

The image shows two terminal windows side-by-side. The left window is a netcat listener on Kali Linux, with the command `nc -l -p 4546` running. It has received a connection from `127.0.0.1`. The right window is a netcat client on Kali Linux, connected to the listener. It has run `ls`, showing the contents of the local directory: `Documents`, `Downloads`, `file0`, `Music`, `Pictures`, `Public`, `Templates`, and `Videos`. The output is displayed in a table-like format with columns for file type, name, and size.