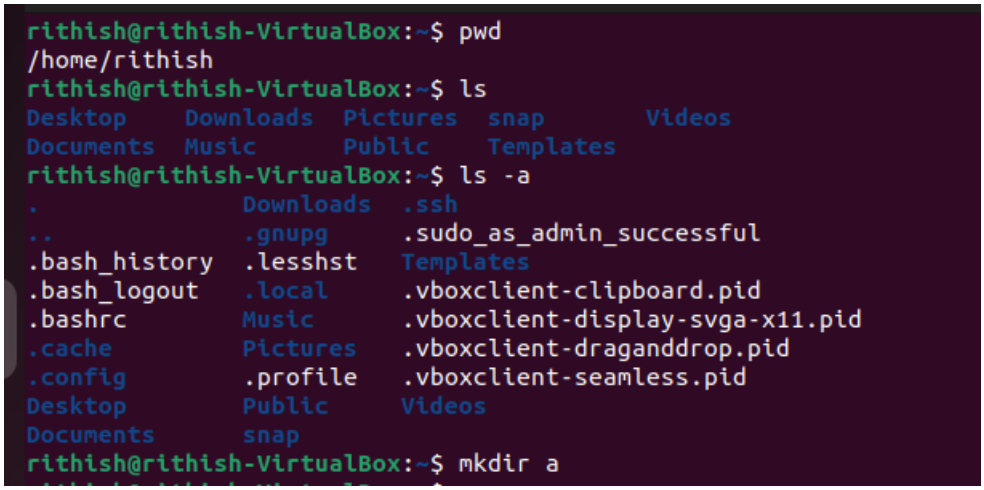
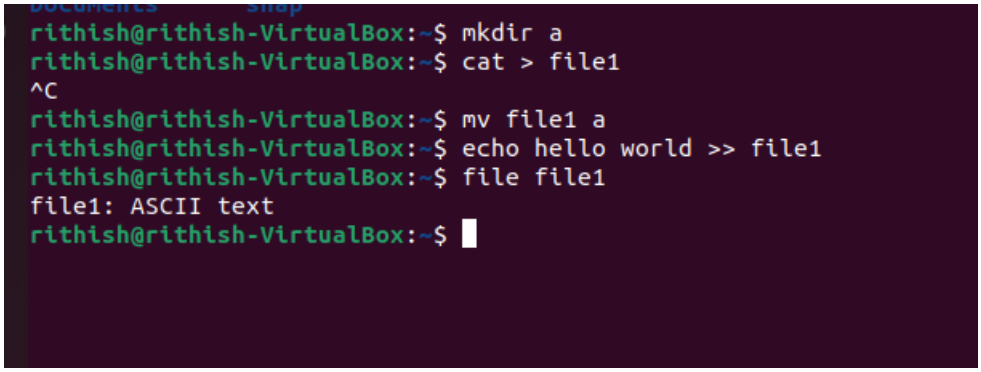
BASH CHALLENGE

PENTEST

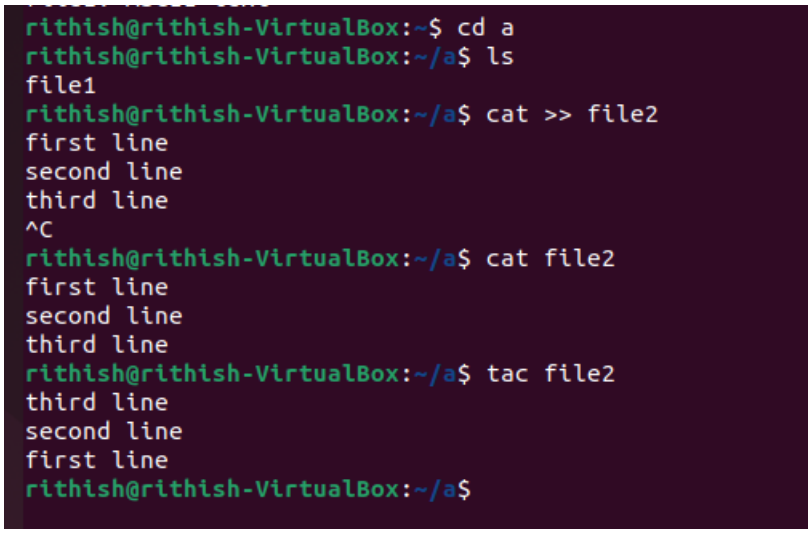
1.



2.



3.



4.

```
rithish@rithish-VirtualBox:~/a$ cat file1 >> file2
rithish@rithish-VirtualBox:~/a$ ls
file1  file2
rithish@rithish-VirtualBox:~/a$ cat file2
first line
second line
third line
rithish@rithish-VirtualBox:~/a$ cat file1
rithish@rithish-VirtualBox:~/a$ echo helloworld >> file1
rithish@rithish-VirtualBox:~/a$ cat file1
helloworld
rithish@rithish-VirtualBox:~/a$ cat file1 >> file2
rithish@rithish-VirtualBox:~/a$ cat file2
first line
second line
third line
helloworld
rithish@rithish-VirtualBox:~/a$ cat file2 > file3
rithish@rithish-VirtualBox:~/a$ cat file3
first line
second line
third line
helloworld
rithish@rithish-VirtualBox:~/a$
```

5.

```
helloworld
rithish@rithish-VirtualBox:~/a$ mkdir b c
rithish@rithish-VirtualBox:~/a$ mkdir d
rithish@rithish-VirtualBox:~/a$ cd c
rithish@rithish-VirtualBox:~/a/c$ pwd
/home/rithish/a/c
rithish@rithish-VirtualBox:~/a/c$ cp d /home/rithish/a/c
cp: cannot stat 'd': No such file or directory
rithish@rithish-VirtualBox:~/a/c$ cd..
cd..: command not found
rithish@rithish-VirtualBox:~/a/c$ cd ..
rithish@rithish-VirtualBox:~/a$ cp d /home/rithish/a/c
cp: -r not specified; omitting directory 'd'
rithish@rithish-VirtualBox:~/a$ cp -r d /home/rithish/a/c
rithish@rithish-VirtualBox:~/a$ rmdir d
rithish@rithish-VirtualBox:~/a$ cp -r file3 /home/rithish/a/c/d
rithish@rithish-VirtualBox:~/a$ cd c
rithish@rithish-VirtualBox:~/a/c$ cd d
rithish@rithish-VirtualBox:~/a/c/d$ cat file3
first line
second line
third line
helloworld
rithish@rithish-VirtualBox:~/a/c/d$
```

6.

```
helloworld
rithish@rithish-VirtualBox:~/a/c/d$ mv file3 file0
rithish@rithish-VirtualBox:~/a/c/d$ ls
file0
rithish@rithish-VirtualBox:~/a/c/d$ mv -r file0 /home/rithish/a
mv: invalid option -- 'r'
Try 'mv --help' for more information.
rithish@rithish-VirtualBox:~/a/c/d$ mv  file0 /home/rithish/a
rithish@rithish-VirtualBox:~/a/c/d$ ls
rithish@rithish-VirtualBox:~/a/c/d$ cd ..
rithish@rithish-VirtualBox:~/a/c$ cd ..
rithish@rithish-VirtualBox:~/a$ ls
b  c  file0  file1  file2  file3
rithish@rithish-VirtualBox:~/a$
```

7.

```
rithish@rithish-VirtualBox:~/a$ cd ~
rithish@rithish-VirtualBox:~$ cat test
cat: test: No such file or directory
rithish@rithish-VirtualBox:~$ cat >> test
^C
rithish@rithish-VirtualBox:~$ pwd test
/home/rithish
rithish@rithish-VirtualBox:~$
```

8.

```
/home/rithish
rithish@rithish-VirtualBox:~$ man grep >> grepman.txt
rithish@rithish-VirtualBox:~$ cat grepman
cat: grepman: No such file or directory
rithish@rithish-VirtualBox:~$ cat grepman.txt
GREP(1)                          User Commands                          G

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

SYNOPSIS
```

```
rithish@rithish-VirtualBox:~$ grep -w FILE grepman.txt
       grep [OPTION...] PATTERNS [FILE...]
       grep [OPTION...] -e PATTERNS ... [FILE...]
       grep [OPTION...] -f PATTERN_FILE ... [FILE...]
       grep  searches  for PATTERNS in each FILE.  PATTERNS is one or more patterns separated
       A  FILE  of  “-”  stands  for standard input.  If no FILE is given, recursive searches
       -f FILE, --file=FILE
              Obtain patterns from FILE, one per line.  If this option is used multiple times
       --exclude-from=FILE
              Skip files whose base name matches any of the file-name globs  read  from  FILE
rithish@rithish-VirtualBox:~$
```

9.

Rm -rf * file

10.

```
rithish@rithish-VirtualBox:~/window$ tat -xvf Files.tar.gz
Command 'tat' not found, but there are 16 similar ones.
rithish@rithish-VirtualBox:~/window$ tar  -xvf Files.tar.gz
tar: Files.tar.gz: Cannot open: No such file or directory
tar: Error is not recoverable: exiting now
rithish@rithish-VirtualBox:~/window$ tar -xvzf  Filez.tar.gz
Filez/
Filez/Flag.txt
rithish@rithish-VirtualBox:~/window$ cat files.txt
cat: files.txt: No such file or directory
rithish@rithish-VirtualBox:~/window$ cat Filez/files.txt
cat: Filez/files.txt: No such file or directory
rithish@rithish-VirtualBox:~/window$ cd Filez
rithish@rithish-VirtualBox:~/window/Filez$ cd
rithish@rithish-VirtualBox:~$ cat Flag.txt
cat: Flag.txt: No such file or directory
rithish@rithish-VirtualBox:~$ cd ..
rithish@rithish-VirtualBox:/home$ ls
rithish
rithish@rithish-VirtualBox:/home$ cd window
bash: cd: window: No such file or directory
rithish@rithish-VirtualBox:/home$ cd ~
rithish@rithish-VirtualBox:~$ cd window
rithish@rithish-VirtualBox:~/window$ ls
Filez  Filez.tar.gz
rithish@rithish-VirtualBox:~/window$  cd Filez
rithish@rithish-VirtualBox:~/window/Filez$ ls
Flag.txt
rithish@rithish-VirtualBox:~/window/Filez$  cat Flag.txt
WW91IEZvdW5kIFRoZSBGbGFnLg==

rithish@rithish-VirtualBox:~/window/Filez$ ^C
rithish@rithish-VirtualBox:~/window/Filez$
```

11.

```
rithish@rithish-VirtualBox:~/window/Filez$ wget logo.png https://blog.bi0s.in/
--2022-10-16 21:09:42--  http://logo.png/
Resolving logo.png (logo.png)... failed: Name or service not known.
wget: unable to resolve host address ‘logo.png’
--2022-10-16 21:09:42--  https://blog.bi0s.in/
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: unspecified [text/html]
Saving to: ‘index.html’

index.html                [  <=>                          ]  26.49K  52.4KB/s    in 0.5s

2022-10-16 21:09:44 (52.4 KB/s) - ‘index.html’ saved [27127]

FINISHED --2022-10-16 21:09:44--
Total wall clock time: 2.0s
Downloaded: 1 files, 26K in 0.5s (52.4 KB/s)
```

```
</html>
rithish@rithish-VirtualBox:~/window/Filez$ curl -o  logo.png https://blog.bi0s.in/
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 27127    0 27127    0     0  16446      0 --:--:--  0:00:01 --:--:-- 16440
rithish@rithish-VirtualBox:~/window/Filez$
```

12.

```
rithish@rithish-VirtualBox:~/window/Filez$ ping -c 5 google.com
PING google.com (142.250.196.14) 56(84) bytes of data.
64 bytes from maa03s44-in-f14.1e100.net (142.250.196.14): icmp_seq=1 ttl=116 time=20.8 ms
64 bytes from maa03s44-in-f14.1e100.net (142.250.196.14): icmp_seq=2 ttl=116 time=20.5 ms
64 bytes from maa03s44-in-f14.1e100.net (142.250.196.14): icmp_seq=3 ttl=116 time=19.5 ms
64 bytes from maa03s44-in-f14.1e100.net (142.250.196.14): icmp_seq=4 ttl=116 time=21.7 ms
64 bytes from maa03s44-in-f14.1e100.net (142.250.196.14): icmp_seq=5 ttl=116 time=38.6 ms

--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 19.546/24.234/38.614/7.223 ms
rithish@rithish-VirtualBox:~/window/Filez$ ping -c 6 -q  google.com
PING google.com (142.250.196.14) 56(84) bytes of data.

--- google.com ping statistics ---
6 packets transmitted, 5 received, 16.6667% packet loss, time 5031ms
rtt min/avg/max/mdev = 19.765/22.208/27.914/3.081 ms
rithish@rithish-VirtualBox:~/window/Filez$
```

13.

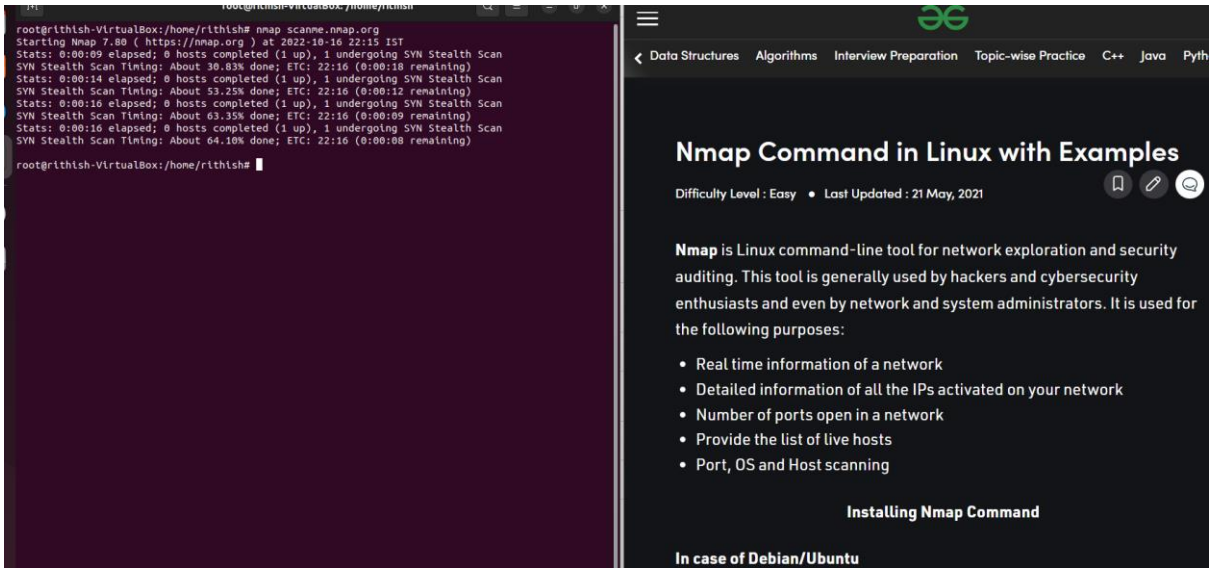
```
rithish@rithish-VirtualBox:~$ ssh bandit0@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


                      This is an OverTheWire game server.
            More information on http://www.overthewire.org/wargames

bandit0@bandit.labs.overthewire.org's password:

      ,-----.           ,----,          .----.
     /   /   \        ,/   .`|         /. ./|
    /   .     :      ,`   .'  :     .--'.  ' ;
   .   /   ;.  \   ;    ;     /    /__./ \ : |
  .   ;   /  ` ; .'___,/    ,' .--'.   '   \' .
  ;   |  ; \ ; | |    :     | /___/ \ |    ' '
  |   :  | ; | ' ;    |.';  ; ;   \  \;      :
  .   |  ' ' ' : `----'  |  |  \   ;  `      |
  '   ;  \; /  |      '   :  ;   .   \    .\  ;
   \   \  ',  /       |   |  '    \   \   ' \ |
    ;   :    /        '   :  |     :   '  |--"
     \   \ .'         ;   |.'       \   \ ;
  www. `---` ver      '---' he        '---" ire.org


Welcome to OverTheWire!

If you find any problems, please report them to the #wargames channel on
discord or IRC.

--[ Playing the games ]--

  This machine might hold several wargames.
  If you are playing "somegame", then:
```

14.

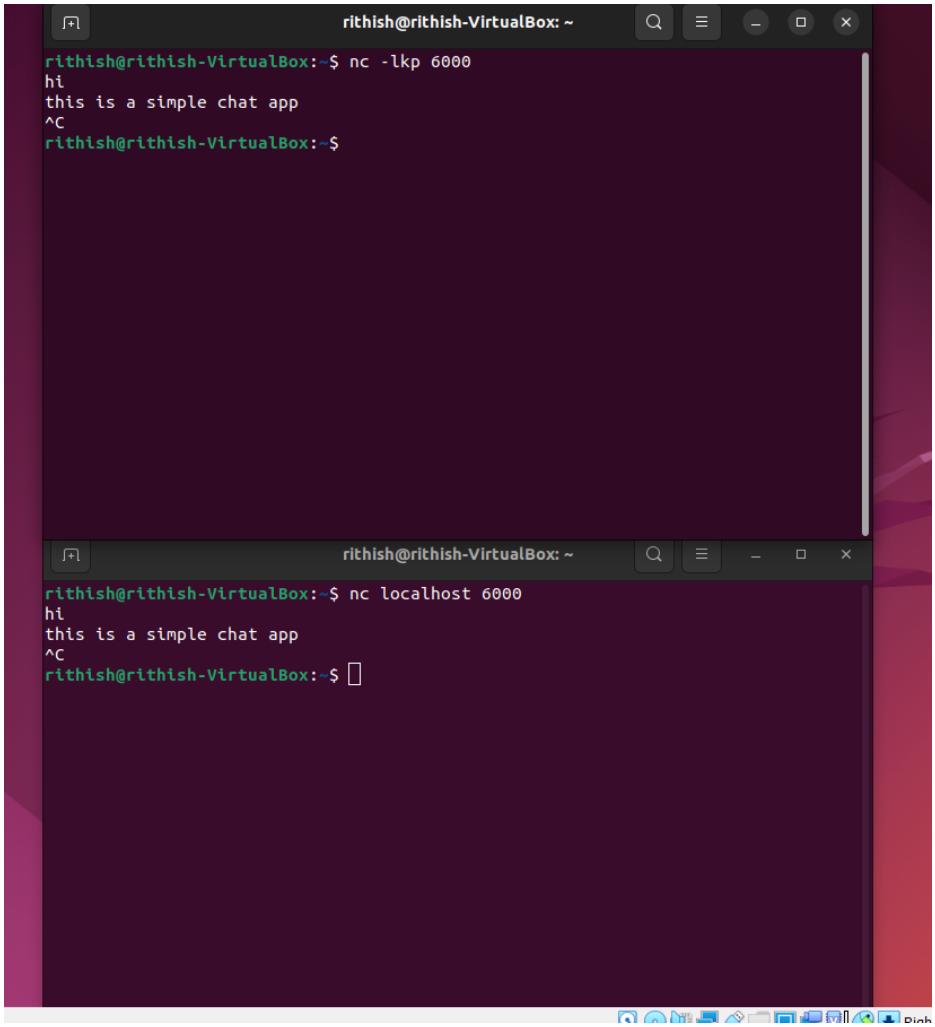
```
rithish@rithish-VirtualBox:~$ telnet localhost
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Ubuntu 22.04.1 LTS
rithish-VirtualBox login: rithish
Password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-50-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

105 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Last login: Mon Oct 17 15:51:45 IST 2022 from localhost on pts/2
rithish@rithish-VirtualBox:~$
```

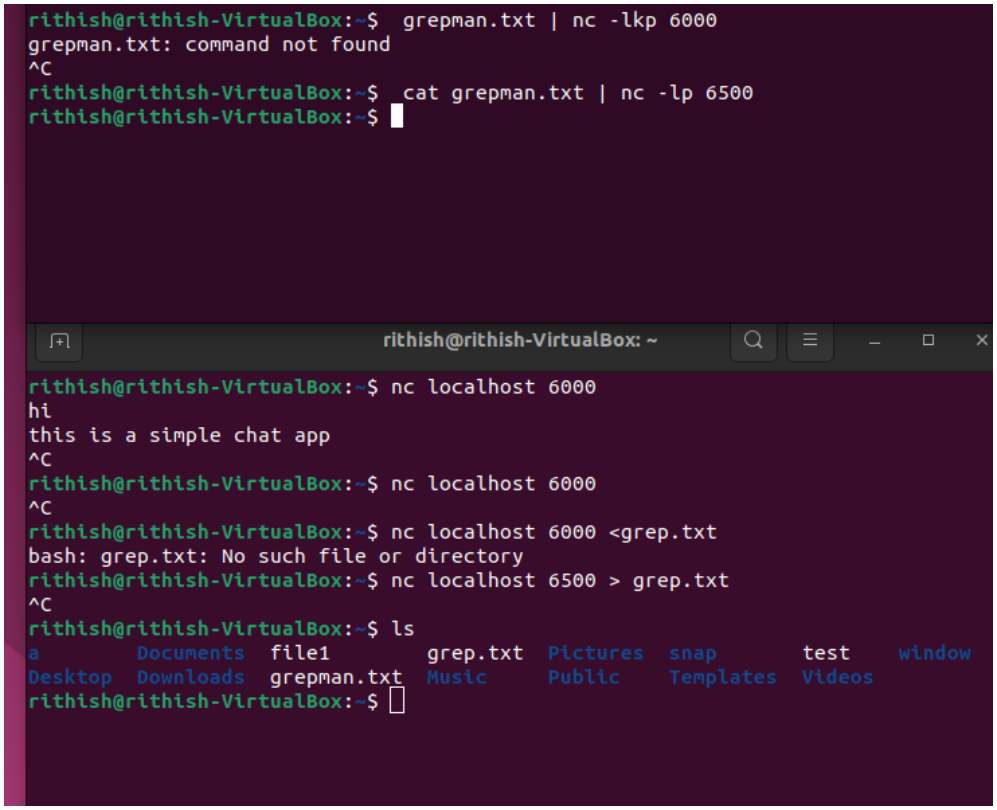
15.

```
Nmap scan report for rithish-VirtualBox (127.0.1.1)
Host is up (0.0000020s latency).
All 1000 scanned ports on rithish-VirtualBox (127.0.1.1) are closed

Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds
root@rithish-VirtualBox:/home/rithish#
```



16.


rithish@rithish-VirtualBox: ~
rithish@rithish-VirtualBox:~$ nc -lkp 6000
hi
this is a simple chat app
^C
rithish@rithish-VirtualBox:~$
rithish@rithish-VirtualBox: ~
rithish@rithish-VirtualBox:~$ nc localhost 6000
hi
this is a simple chat app
^C
rithish@rithish-VirtualBox:~$


rithish@rithish-VirtualBox:~$ grepman.txt | nc -lkp 6000
grepman.txt: command not found
^C
rithish@rithish-VirtualBox:~$ cat grepman.txt | nc -lp 6500
rithish@rithish-VirtualBox:~$
rithish@rithish-VirtualBox: ~
rithish@rithish-VirtualBox:~$ nc localhost 6000
hi
this is a simple chat app
^C
rithish@rithish-VirtualBox:~$ nc localhost 6000
^C
rithish@rithish-VirtualBox:~$ nc localhost 6000 <grep.txt
bash: grep.txt: No such file or directory
rithish@rithish-VirtualBox:~$ nc localhost 6500 > grep.txt
^C
rithish@rithish-VirtualBox:~$ ls
a Documents file1 grep.txt Pictures snap test window
Desktop Downloads grepman.txt Music Public Templates Videos
rithish@rithish-VirtualBox:~$

Shell scripting

1

```
#!/bin/bash
echo "simple calculator"
res=0
i="y"
echo "enter first number"
read a
echo "enter second number"
read b
while [ $i = "y" ]
do
echo "1.add"
echo "2.subract"
echo "3.multiply"
echo "4.divide"
read ch
case $ch in
1)res=$(echo "$a + $b" | bc -l )
echo "addition is =" $res;;
2)res=$(echo "$a - $b" | bc -l )
echo "sub is =" $res;;
3)res=$(echo "$a * $b" | bc -l )
echo "mul is =" $res;;
4)res=$(echo "$a / $b" | bc -l )
echo "div is =" $res;;
*) echo "invalid choice:"
esac
echo " do you want to continue"
read i
if [ $i != "y" ]
then
exit
fi
done


```

```
rithish@rithish-VirtualBox:~$ gedit script.sh
rithish@rithish-VirtualBox:~$ ./script.sh
simple calculator
enter first number
2
enter second number
2
1.add
2.subract
3.multiply
4.divide
1
addition is = 4
 do you want to continue
n
rithish@rithish-VirtualBox:~$
```

2.

```
1 read n
2 echo $n
3 echo "1. for encypt"
4 echo "2. for decrypt"
5 read i
6 if [ $i -eq 1 ];
7 then
8 echo $n
9 ch=$(echo $n | tr 'A-Za-z' 'N-ZA-Mn-za-m')
0 echo $ch
1 elif [ $i -eq 2 ];
2 then
3 rv=$(echo $n | tr 'A-Za-z' 'N-ZA-Mn-za-m')
4 echo  $rv
5 else
6 echo "not crt"
7 fi
8
9
```

```
└─# ./rot.sh
rithish
rithish
1. for encypt
2. for decrypt
1
rithish
evguvfu
┌─[root@parrot]─[~]
└──#
```

4.

```
GNU nano 5.4
#!/bin/bash
echo "enter maximum number"
read n
echo "enter Numbers in array:"
for (( i = 0; i < $n; i++ ))
do
read nos[$i]
done
for (( i = 0; i < $n ; i++ ))
do
for (( j = $i; j < $n; j++ ))
do
if [ ${nos[$i]} -gt ${nos[$j]}  ]; then
t=${nos[$i]}
nos[$i]=${nos[$j]}
nos[$j]=$t
fi
done
done
echo -e "\nSorted Numbers "
for (( i=0; i < $n; i++ ))
do
echo ${nos[$i]}
done
```

```
└──╼ #./sor.sh
enter maximum number
5
enter Numbers in array:
4
5
3
4
5

Sorted Numbers
3
4
4
5
5
┌─[root@parrot]─[~]
└──╼ #
```

5

```
#!/bin/bash
echo 'enter n'
read n
rev=$(echo $n | rev)
if [ $n -eq $rev ]; then
   echo "number is palindrome"
else
   echo "number is not palindrome"
fi
```