QUESTION 1

```
ajay@ajay-VirtualBox:~$ gcalccmd
> 5+10
15
> 5*10
50
> 7/2
3.5
> 10-15
-  5
```

QUESTION 2

```
ajay@ajay-VirtualBox:~$ gedit new.c
echo “Enter the limit:”

read n

echo “Enter the numbers”

for(( i=0 ;i<n; i++ ))

do

read m

a[i]=$m

done

for(( i=1; i<n; i++ ))

do

for(( j=0; j<n-i; j++))

do

if [ ${a[$j]} -gt ${a[$j+1]} ]

then

t=${a[$j]}

a[$j]=${a[$j+1]}

a[$j+1]=$t

fi
```

```
done
done
echo “Sorted array is”
for(( i=0; i<n; i++ ))
do
echo “${a[$i]}”
done
echo “Enter the element to be searched :”
read s
l=0
c=0
u=$(($n-1))
while [ $l -le $u ]
do
mid=$(((( $l+$u ))/2 ))
if [ $s -eq ${a[$mid]} ]
then
c=1
break
elif [ $s -lt ${a[$mid]} ]
then
u=$(($mid-1))
else
l=$(($mid+1))
fi
done
if [ $c -eq 1 ]
```

```
then

echo “Element found at position $(($mid+1))”

else

echo “Element not found”
```

QUESTION 3

Commands used for finding memory usage are

1. free command
The free command is the most simple and easy to use command to check memory usage on linux.

2. /proc/meminfo
The next way to check memory usage is to read the /proc/meminfo file. Know that the /proc file system does not contain real files. They are rather virtual files that contain dynamic information about the kernel and the system.

3. vmstat
The vmstat command with the s option, lays out the memory usage statistics much like the proc command.

4. top command
The top command is generally used to check memory and cpu usage per process. However it also reports total memory usage and can be used to monitor the total RAM usage. The header on output has the required information.

5. htop
Similar to the top command, the htop command also shows memory usage along with various other details.

QUESTION 4

```
ajay@ajay-VirtualBox:~$ cd parent
ajay@ajay-VirtualBox:~/parent$ cd child
ajay@ajay-VirtualBox:~/parent/child$ ls
michel  watson  white
ajay@ajay-VirtualBox:~/parent/child$ ls --file-type *.txt
ls: cannot access '*.txt': No such file or directory
```

```
ajay@ajay-VirtualBox:~/parent/child$ cat >> y.txt
bfwhwhbgiuser@ajay-VirtualBox:~/parent/child$ ls
michel  watson  white  y.txt
ajay@ajay-VirtualBox:~/parent/child$ ls --file-type *.txt
y.txt
ajay@ajay-VirtualBox:~/parent/child$ cat >> a.txt
qbgdjkduser@ajay-VirtualBox:~/parent/child$ cat >> b.cpp
akfhioauser@ajay-VirtualBox:~/parent/child$ cat >> c.cpp
hifgiouser@ajay-VirtualBox:~/parent/child$ cat >> d.exe
whfiwhfo
ajay@ajay-VirtualBox:~/parent/child$ cat >> e.exe
bihgqiuuser@ajay-VirtualBox:~/parent/child$ ls --file-type *.txt
a.txt  y.txt
ajay@ajay-VirtualBox:~/parent/child$ ls --file-type *.exe
d.exe  e.exe
ajay@ajay-VirtualBox:~/parent/child$ ls --file-type *.cpp
b.cpp  c.cpp
```

QUESTION 5

```
ajay@ajay-VirtualBox:~$ mkdir dir1
ajay@ajay-VirtualBox:~$ cd dir1
ajay@ajay-VirtualBox:~/dir1$ mkdir dir2
ajay@ajay-VirtualBox:~/dir1$ cd dir2
ajay@ajay-VirtualBox:~/dir1/dir2$ cd ../..
ajay@ajay-VirtualBox:~$
```

QUESTION 6

Linux is very simple but still very secure operating system, which protects the important files from the attack of viruses and malware. So, if you are wondering how Linux is more secure than the giant operating systems, like iOS, Windows, and Android, then to better understand this, look at few advantages of Linux security.
some parameters which make linux more secure than other operating system

1. A perk of Accounts.

In the operating system such as Windows, users have full admin access to the accounts of software. When the virus strikes in this system and then within few seconds it corrupts the whole system. In short, all the files are in danger due to the open access, but in the Linux, very low access is

given to the users. Thus the viruses can’t attack the whole system and they only attack few files, and other system works without any issue.

2. Strong Community.

Windows and other operating systems are more vulnerabilities to the type of social engineering Ltd compared to Linux. Amateur users can easily expose to the viruses in other OS by opening one email. But this is not the case in the Linux and user needs full execution right before opening any new attachment. Thus web developers and testers prefer this system as it saves them from the vulnerabilities.

3. IPtables.

A high tech security of IPtables is used by the Linux to enhance the security circle of the system. This firewall that allows you to create a more secure environment for the execution of any command or access the network.

4. Different working environment.

Linux system operates in the different environment such as such as Linux Mint, Debian, Ubuntu, Gentoo, Arch, and many others. The division and segmented working environment protect from the attack of the virus. On the other hand, Windows isn’t much divided operating system and thus it is more exposed to the threats.

5. Recording in Linux.

A Proper log is established in the Linux of the timing and it can be viewed later on easily. If someone tries to enter safe system files, these system gaps can be viewed by the system administrator. Also, the disk to fail attempts are presented to read for later on.

QUESTION 7

```
ajay@ajay-VirtualBox:~$ gedit new.c
                        #include<stdio.h>
                        int main()
                        {
                                int num,sum=0,i=1;
                                printf("Enter number\n");
                                scanf("%d",&num);
                                if(num<0)
                                num=num-(num*2);
                                while(num!=0)
                                {
                                   sum+=(num%8)*i;
                                   num=num/8;
                                   i*=10;
                                }
```

```
                                printf("%d",sum);
                                return 0;
                        }
ajay@ajay-VirtualBox:~$ gcc -o new new.c
ajay@ajay-VirtualBox:~$ ./new
Enter number
15
17
```

QUESTION 8

```
ajay@ajay-VirtualBox:~$ sudo chroot /media/linx_part/
root@ajay-VirtualBox:/# passwd
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@ajay-VirtualBox:/# exit
exit
ajay@ajay-VirtualBox:~$
```

QUESTION 9

(1).

```
$find . -name '*.c' -or -name '*.cpp'
```

(2).

In computing, umask is a command that determines the settings of a mask that controls how file permissions are set for newly created files. In one case it also influences how the file permissions are changed explicitly. umask may also refer to a function that sets the mask, or it may refer to the mask itself, which is formally known as the file mode creation mask. The mask is a grouping of bits, each of which restricts how its corresponding permission is set for newly created files. The bits in the mask may be changed by invoking the umask command.

In UNIX, each file has a set of attributes that control who can read, write or execute it. When a program creates a file, UNIX requires that the file permissions be set to an initial setting. The mask restricts permission settings. If the mask has a bit set to "1", it means that the corresponding initial file permission will be disabled. A bit set to "0" in the mask means that the corresponding permission will be determined by the program and the system. In other words, the mask acts as a last-stage filter that strips away permissions as a file is created; each bit that is set to a "1" strips away its corresponding permission. Permissions may be changed later by users and programs using chmod.

(3).

```
        ajay@ajay-VirtualBox:~$ cd parent
      ajay@ajay-VirtualBox:~/parent$ cd child
      ajay@ajay-VirtualBox:~/parent/child$ ls
```

```
a.txt  b.cpp  c.cpp  d.exe  e.exe  michel  watson  white  y.txt
ajay@ajay-VirtualBox:~/parent/child$ cd ..
ajay@ajay-VirtualBox:~/parent$ rmdir -r child
rmdir: invalid option -- 'r'
Try 'rmdir --help' for more information.
ajay@ajay-VirtualBox:~/parent$ cd ..
ajay@ajay-VirtualBox:~$ rmdir -r parent
rmdir: invalid option -- 'r'
Try 'rmdir --help' for more information.
ajay@ajay-VirtualBox:~$ pwd
/home/user
ajay@ajay-VirtualBox:~$ rmdir -r /home/user/parent
rmdir: invalid option -- 'r'
Try 'rmdir --help' for more information.
ajay@ajay-VirtualBox:~$ rm -r parent
ajay@ajay-VirtualBox:~$
```