

# Information Security

## Lab – 1

Name: Atmik Ajoy

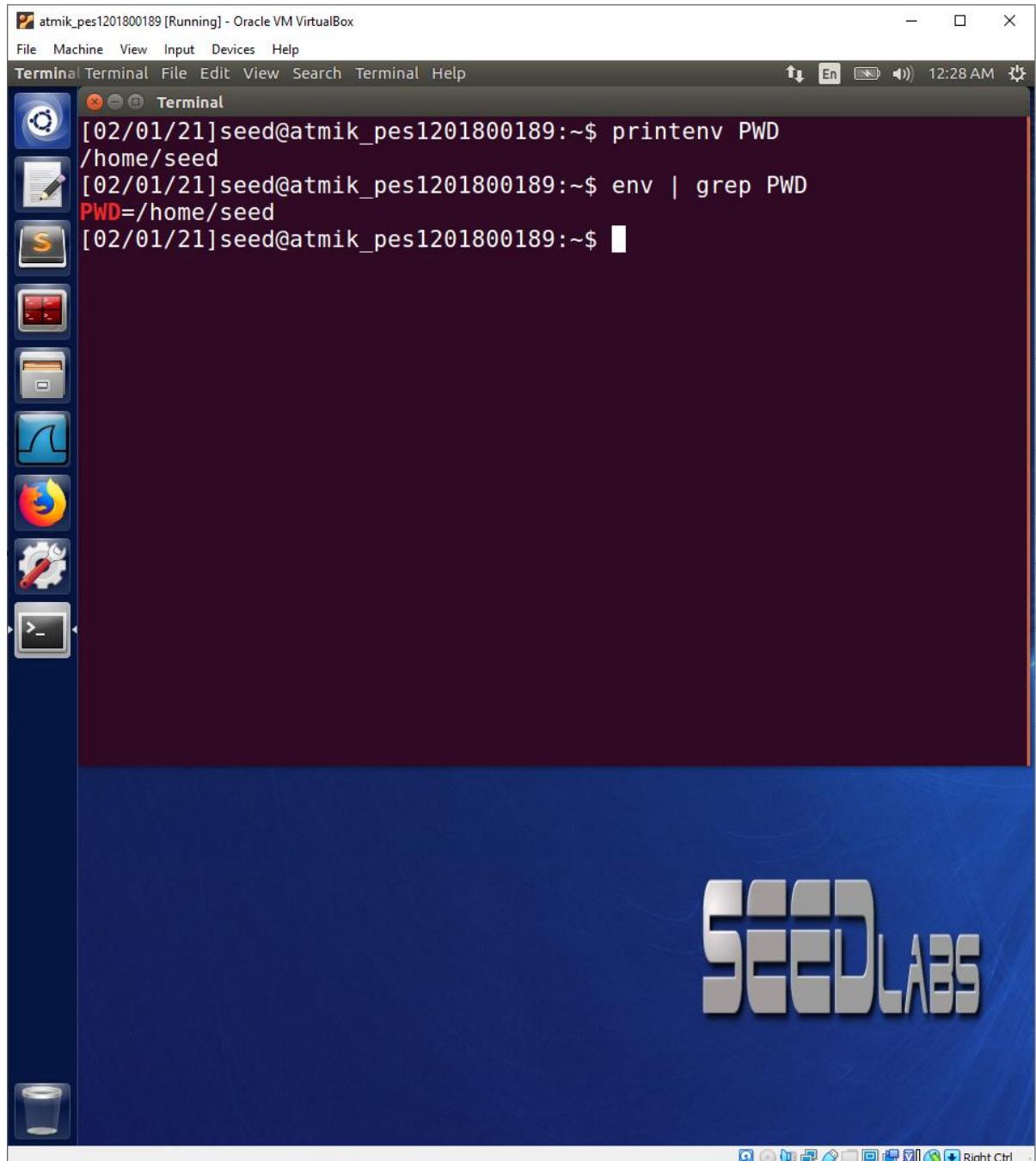
SRN: PES1201800189

Section – A

## Task1

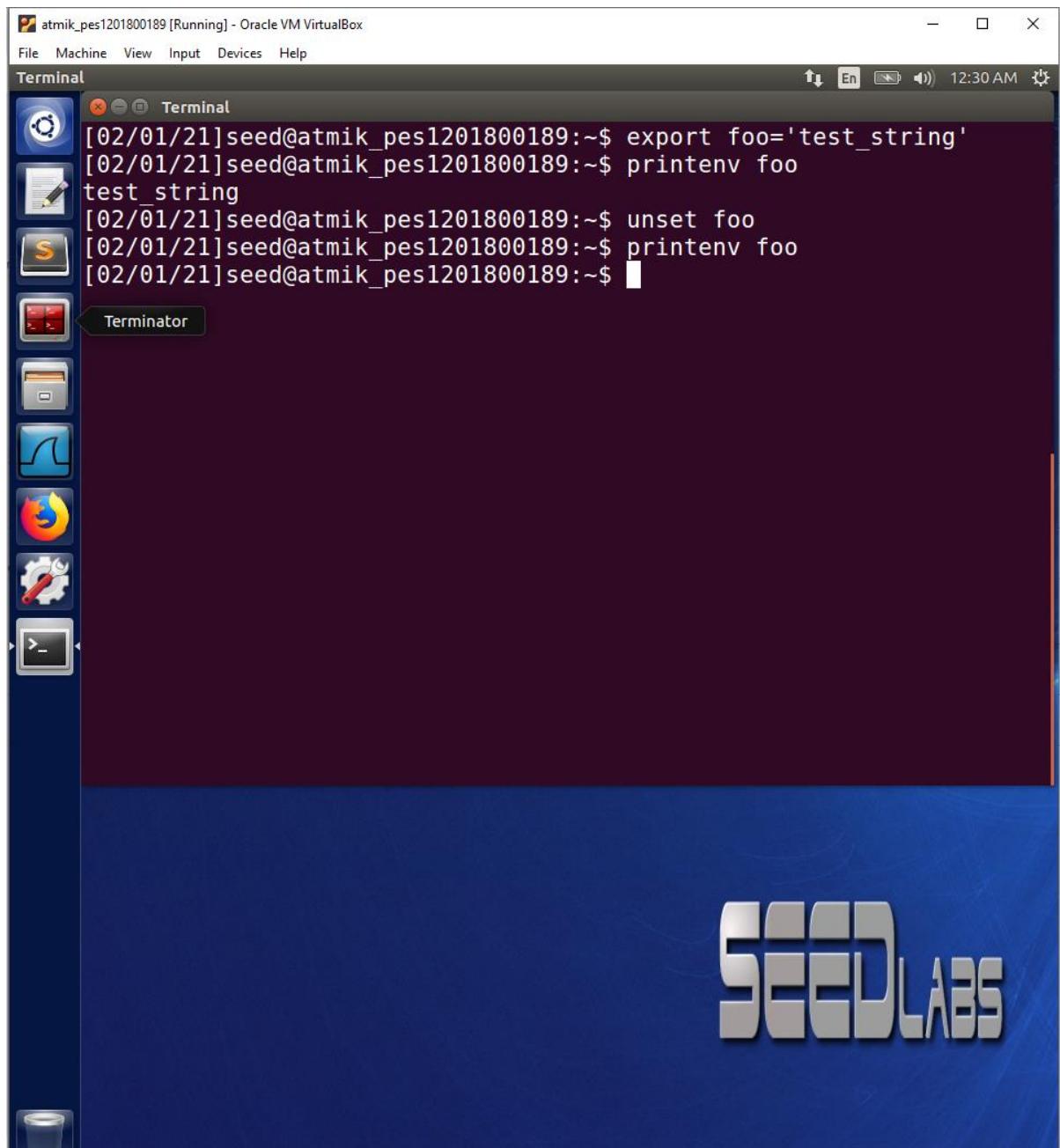
### Step1

- `printenv *variable_name*` prints the value of the environment variable
- `printenv PWD` prints the value of the current working directory which in our case is `/home/seed`



## Step 2

- the export command is used to set a variable in the current shell and for all the processes running in said shell, here we have created a variable foo and set it to 'test\_string'
- the unset command is used to clear the variable that we just set (using export), here we unset foo and hence when we printenv after export it prints the string stored but after unsetting its empty



## TASK 2

- values of environment variables for child are stored in child and same for parent
- diff child parent shows that all the environmental variables are inherited by child process
- but each process has its own environment hence, any changes made in environment variables will not be visible in child and vice versa

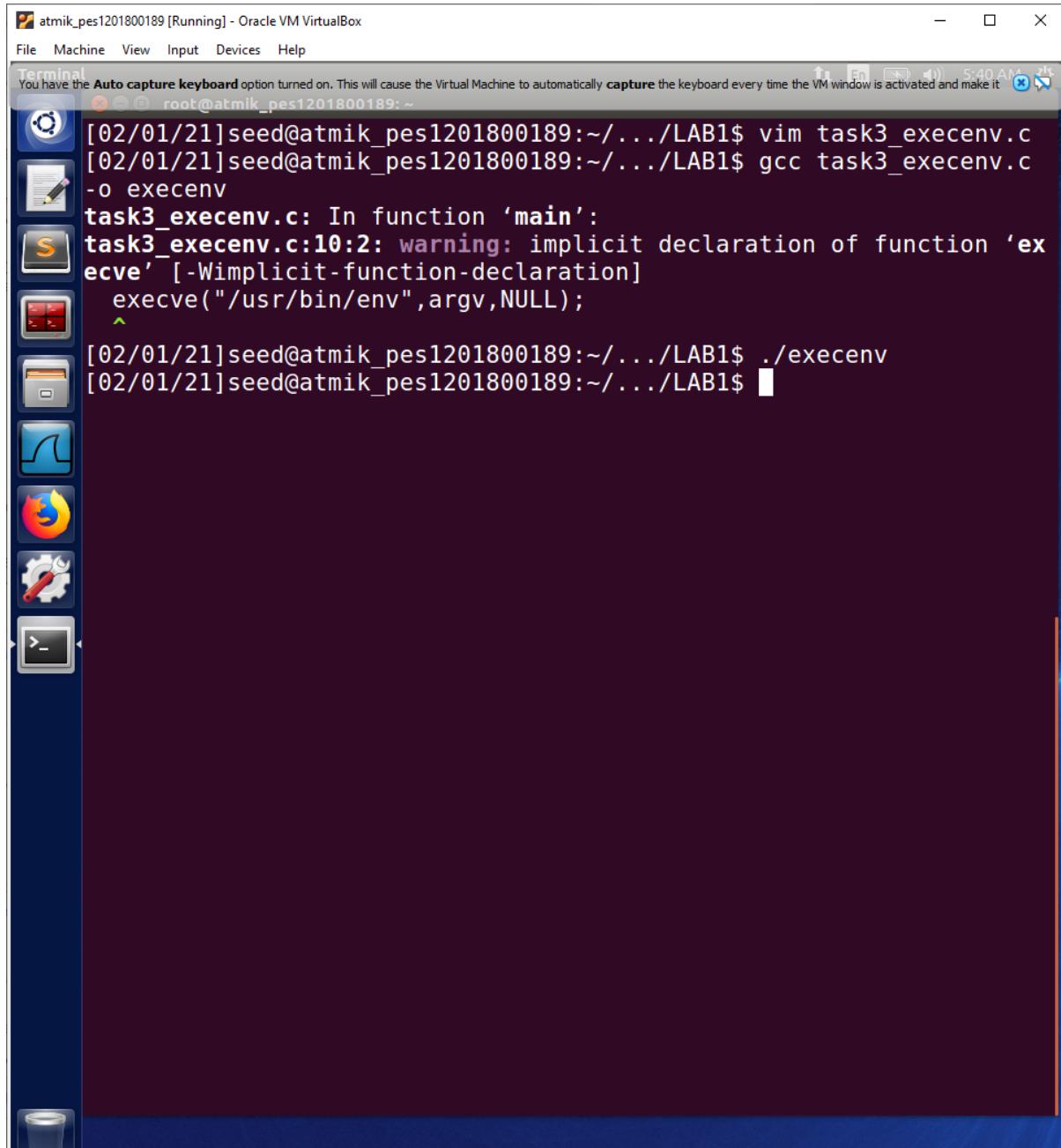
The screenshot shows a Linux desktop environment with a dark theme. A terminal window is open, showing the command-line session below. A file manager window is also visible in the background.

```
[root@atmik_pes1201800189 ~]# gcc task2.c
[02/02/21]seed@atmik_pes1201800189:~/LAB1$ a.out>child
[02/02/21]seed@atmik_pes1201800189:~/LAB1$ ls -l child
-rw-rw-r-- 1 seed seed 3857 Feb  2 04:38 child
[02/02/21]seed@atmik_pes1201800189:~/LAB1$ gcc task2.c
[02/02/21]seed@atmik_pes1201800189:~/LAB1$ a.out>parent
[02/02/21]seed@atmik_pes1201800189:~/LAB1$ ls -l parent
-rw-rw-r-- 1 seed seed 3857 Feb  2 04:38 parent
[02/02/21]seed@atmik_pes1201800189:~/LAB1$ diff child parent
[02/02/21]seed@atmik_pes1201800189:~/LAB1$
```

## Task 3

### Step 1:

- since execve passes NULL to new program , ./execenc doesn't print anything



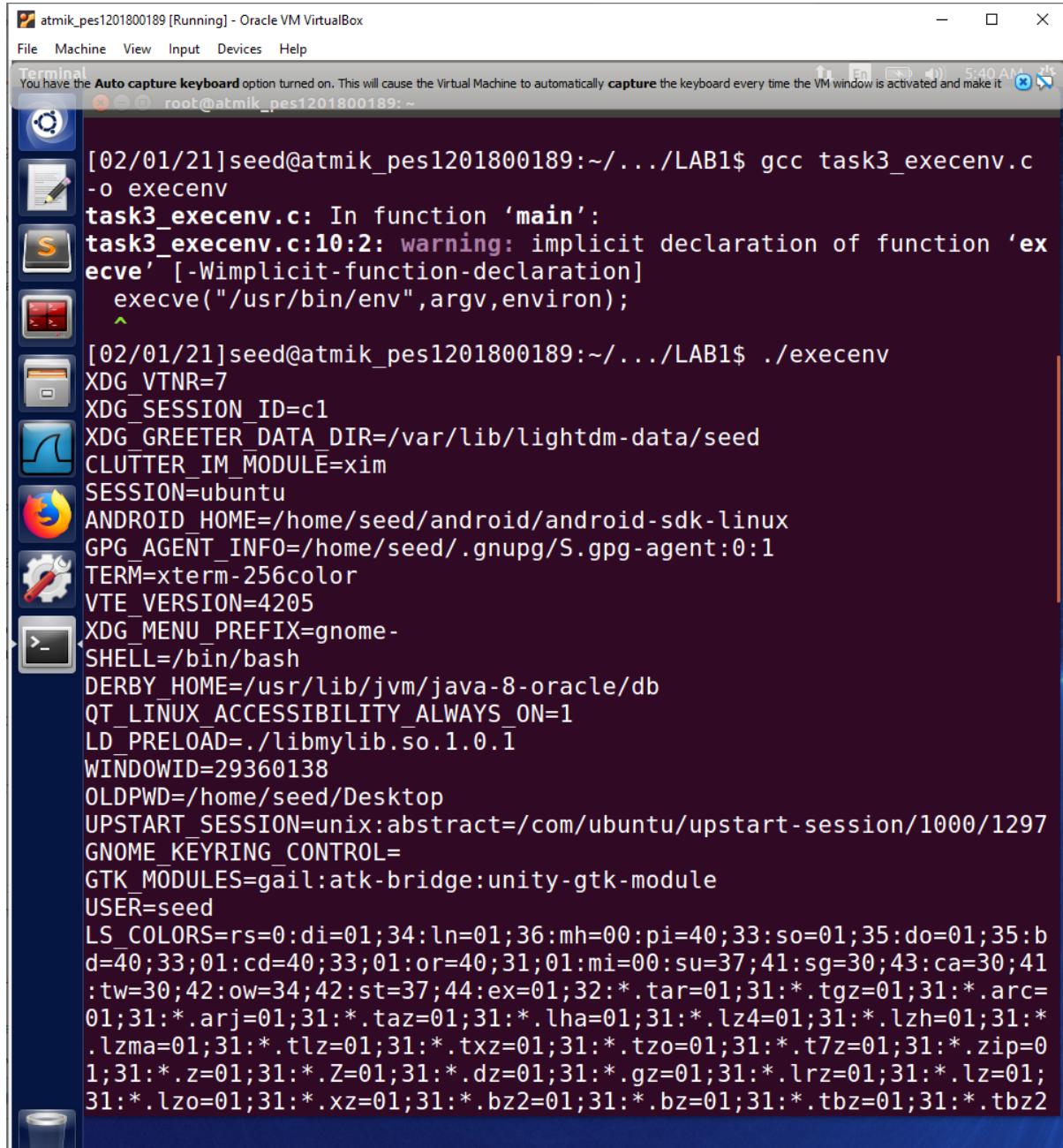
The screenshot shows a terminal window titled "atmik\_pes1201800189 [Running] - Oracle VM VirtualBox". The terminal window has a dark blue background and a light blue header bar. The header bar includes the title, a menu bar with "File", "Machine", "View", "Input", "Devices", and "Help", and a system tray with icons for battery, signal, and volume. The main area of the terminal shows the following command-line session:

```
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ vim task3_execenv.c
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ gcc task3_execenv.c
-o execenv
task3_execenv.c: In function 'main':
task3_execenv.c:10:2: warning: implicit declaration of function 'execve' [-Wimplicit-function-declaration]
    execve("/usr/bin/env", argv, NULL);
               ^
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ ./execenv
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$
```

The terminal window has a vertical scroll bar on the right side. To the left of the terminal window is a docked application bar with several icons: a terminal icon (highlighted), a file manager icon, a browser icon, a settings icon, and a terminal icon.

## Step 2:

- since we pass environ(which is a pointer to a string array having key value pairs of environment variables) to the new program, it prints a full list of env variables acquired by program

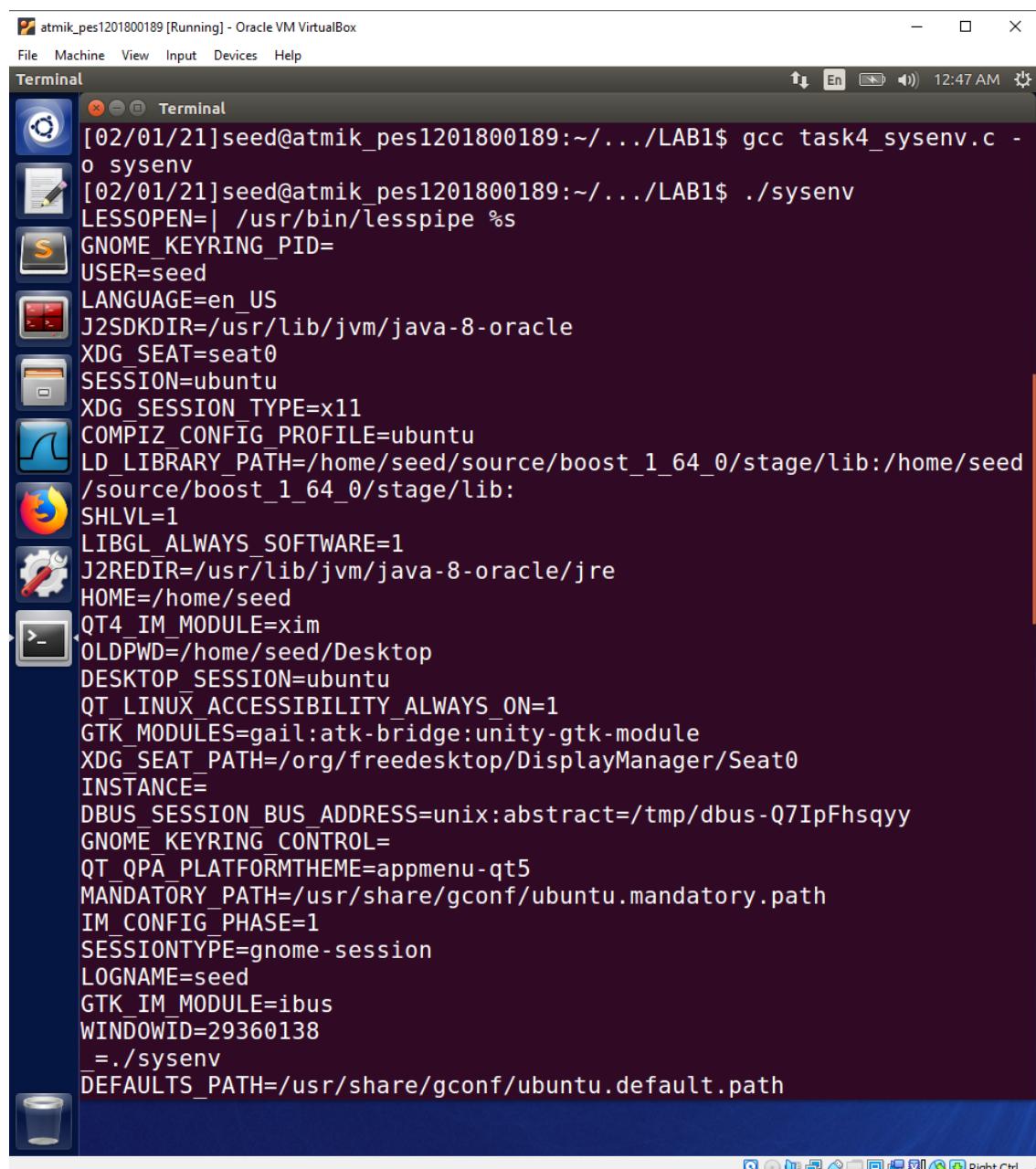


The screenshot shows a terminal window titled "Terminal" running on a Linux desktop. The window title bar says "atmik\_pes1201800189 [Running] - Oracle VM VirtualBox". The terminal window displays the following text:

```
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ gcc task3_execenv.c  
-o execenv  
task3_execenv.c: In function 'main':  
task3_execenv.c:10:2: warning: implicit declaration of function 'execve' [-Wimplicit-function-declaration]  
    execve("/usr/bin/env", argv, environ);  
  
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ ./execenv  
XDG_VTNR=7  
XDG_SESSION_ID=c1  
XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed  
CLUTTER_IM_MODULE=xim  
SESSION=ubuntu  
ANDROID_HOME=/home/seed/android/android-sdk-linux  
GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1  
TERM=xterm-256color  
VTE_VERSION=4205  
XDG_MENU_PREFIX=gnome-  
SHELL=/bin/bash  
DERBY_HOME=/usr/lib/jvm/java-8-oracle/db  
QT_LINUX_ACCESSIBILITY_ALWAYS_ON=1  
LD_PRELOAD=./libmylib.so.1.0.1  
WINDOWID=29360138  
OLDPWD=/home/seed/Desktop  
UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1297  
GNOME_KEYRING_CONTROL=  
GTK_MODULES=gail:atk-bridge:unity-gtk-module  
USER=seed  
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33:01:cd=40;33:01:or=40;31:01:mi=00:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;31:*.lz4=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;31:*.tz=01;31:*.zip=01;31:*.z=01;31:*.Z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.bz2=01;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;
```

## Task 4

- Environment variables of the program is passed to /bin/sh by execve() which is called by execl() and system()
- ./sysenv displays all the environment variables as it runs the executable



The screenshot shows a terminal window titled "Terminal" running on a Linux desktop. The window title bar includes the name of the terminal and the date/time. The terminal itself displays a list of environment variables. The output starts with the command "gcc task4\_sysenv.c -o sysenv" and then lists numerous environment variables such as "LESSOPEN", "GNOME\_KEYRING\_PID", "USER", "LANGUAGE", "J2SDKDIR", "XDG\_SEAT", "SESSION", "XDG\_SESSION\_TYPE", "COMPIZ\_CONFIG\_PROFILE", "LD\_LIBRARY\_PATH", "source/boost\_1\_64\_0/stage/lib:", "SHLVL", "LIBGL\_ALWAYS\_SOFTWARE", "J2REDIR", "HOME", "QT4\_IM\_MODULE", "OLDPWD", "DESKTOP\_SESSION", "QT\_LINUX\_ACCESSIBILITY\_ALWAYS\_ON", "GTK\_MODULES", "XDG\_SEAT\_PATH", "INSTANCE", "DBUS\_SESSION\_BUS\_ADDRESS", "GNOME\_KEYRING\_CONTROL", "QT\_QPA\_PLATFORMTHEME", "MANDATORY\_PATH", "IM\_CONFIG\_PHASE", "SESSIONTYPE", "LOGNAME", "GTK\_IM\_MODULE", "WINDOWID", "DEFAULTS\_PATH". The terminal window has a dark background and light-colored text, with icons for various applications visible along the left edge.

```
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ gcc task4_sysenv.c -o sysenv
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ ./sysenv
LESSOPEN=| /usr/bin/lesspipe %s
GNOME_KEYRING_PID=
USER=seed
LANGUAGE=en_US
J2SDKDIR=/usr/lib/jvm/java-8-oracle
XDG_SEAT=seat0
SESSION=ubuntu
XDG_SESSION_TYPE=x11
COMPIZ_CONFIG_PROFILE=ubuntu
LD_LIBRARY_PATH=/home/seed/source/boost_1_64_0/stage/lib:/home/seed/source/boost_1_64_0/stage/lib:
SHLVL=1
LIBGL_ALWAYS_SOFTWARE=1
J2REDIR=/usr/lib/jvm/java-8-oracle/jre
HOME=/home/seed
QT4_IM_MODULE=xim
OLDPWD=/home/seed/Desktop
DESKTOP_SESSION=ubuntu
QT_LINUX_ACCESSIBILITY_ALWAYS_ON=1
GTK_MODULES=gail:atk-bridge:unity-gtk-module
XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0
INSTANCE=
DBUS_SESSION_BUS_ADDRESS=unix:abstract=/tmp/dbus-Q7IpFhsqyy
GNOME_KEYRING_CONTROL=
QT_QPA_PLATFORMTHEME=appmenu-qt5
MANDATORY_PATH=/usr/share/gconf/ubuntu.mandatory.path
IM_CONFIG_PHASE=1
SESSIONTYPE=gnome-session
LOGNAME=seed
GTK_IM_MODULE=ibus
WINDOWID=29360138
./sysenv
DEFAULTS_PATH=/usr/share/gconf/ubuntu.default.path
```

atmik\_pes1201800189 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal

XDG\_SESSION\_ID=c1  
TERM=xterm-256color  
GNOME\_DESKTOP\_SESSION\_ID=this-is-deprecated  
GTK2\_MODULES=overlay-scrollbar  
PATH=/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/bin:/usr/games:/usr/local/games:./snap/bin:/usr/lib/jvm/java-8-oracle/bin:/usr/lib/jvm/java-8-oracle/db/bin:/usr/lib/jvm/java-8-oracle/jre/bin:/home/seed/android/android-sdk-linux/tools:/home/seed/android/android-ndk/android-ndk-r8d:/home/seed/.local/bin  
DERBY\_HOME=/usr/lib/jvm/java-8-oracle/db  
SESSION\_MANAGER=local/atmik\_pes1201800189:@/tmp/.ICE-unix/1700,unix/atmik\_pes1201800189:/tmp/.ICE-unix/1700  
GDM\_LANG=en\_US  
XDG\_MENU\_PREFIX=gnome-  
XDG\_SESSION\_PATH=/org/freedesktop/DisplayManager/Session0  
XDG\_RUNTIME\_DIR=/run/user/1000  
DISPLAY=:0  
LD\_PRELOAD=/home/seed/lib/boost/libboost\_program\_options.so.1.64.0:/home/seed/lib/boost/libboost\_filesystem.so.1.64.0:/home/seed/lib/boost/libboost\_system.so.1.64.0  
LANG=en\_US.UTF-8  
XDG\_CURRENT\_DESKTOP=Unity  
LS\_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33:01:cd=40;33:01:or=40;31:01:mi=00:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:\*.tar=01;31:\*.tgz=01;31:\*.arc=01;31:\*.arj=01;31:\*.taz=01;31:\*.lha=01;31:\*.lz4=01;31:\*.lzh=01;31:\*.lzma=01;31:\*.tlz=01;31:\*.txz=01;31:\*.tzo=01;31:\*.tz=01;31:\*.zip=01;31:\*.z=01;31:\*.Z=01;31:\*.dz=01;31:\*.gz=01;31:\*.lrz=01;31:\*.lz=01;31:\*.lzo=01;31:\*.xz=01;31:\*.bz2=01;31:\*.bz=01;31:\*.tbz=01;31:\*.tbz2=01;31:\*.tz=01;31:\*.deb=01;31:\*.rpm=01;31:\*.jar=01;31:\*.war=01;31:\*.ear=01;31:\*.sar=01;31:\*.rar=01;31:\*.alz=01;31:\*.ace=01;31:\*.zoo=01;31:\*.cpio=01;31:\*.7z=01;31:\*.rz=01;31:\*.cab=01;31:\*.jpg=01;35:\*.jpeg=01;35:\*.gif=01;35:\*.bmp=01;35:\*.pbm=01;35:\*.pgm=01;35:\*.ppm=01;35:\*.tga=01;35:\*.xbm=01;35:\*.xpm=01;35:\*.tif=01;35:\*.tiff=01;35:\*.png=01;35:\*.svg=01;35:\*.svgz=01;35:\*.mng=01;35:\*.pcx=01;35:\*.mov=01;35:\*

4.2

atmik\_pes1201800189 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal

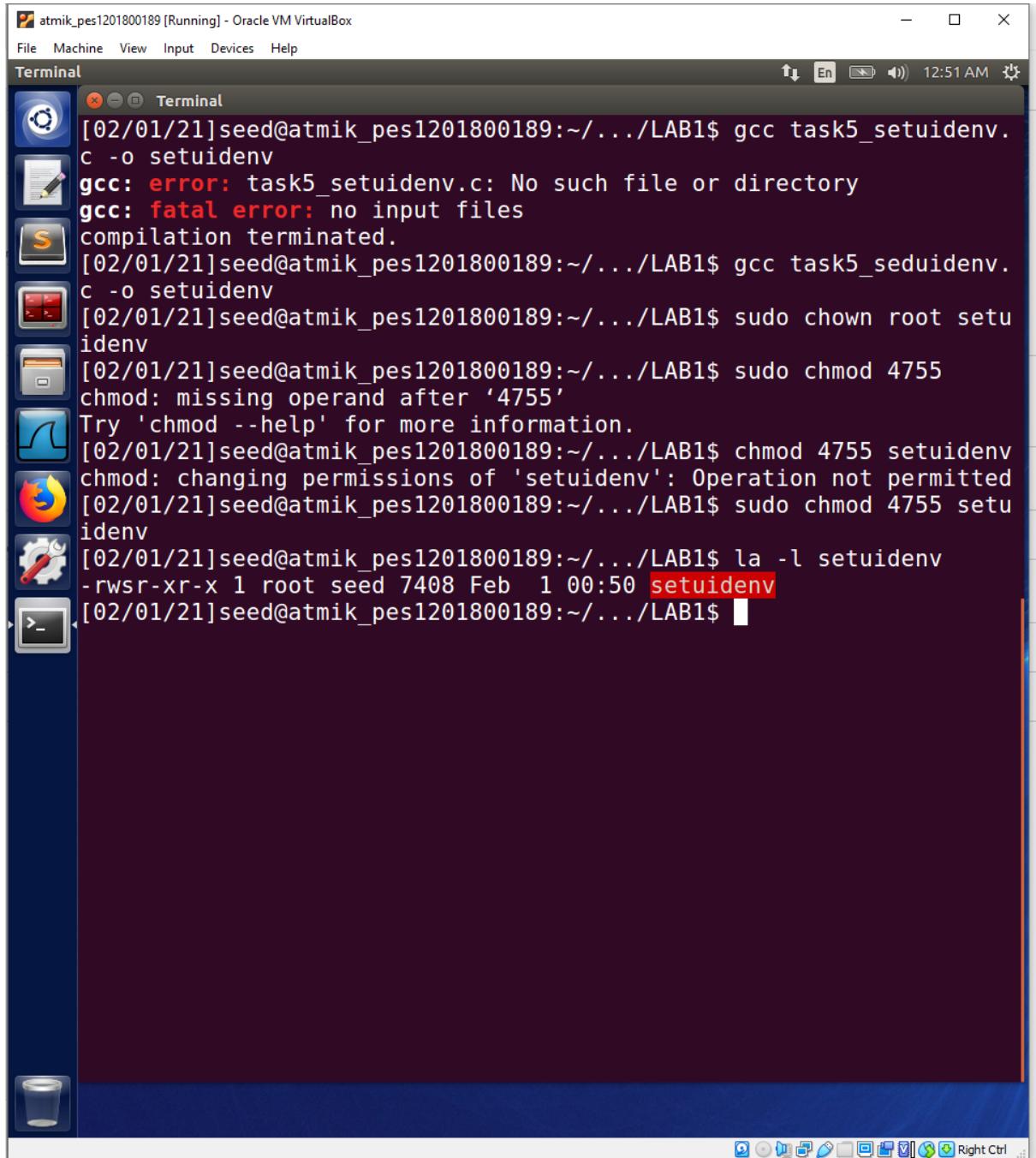
```
;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;31:*.jpg=01;35:*.jp  
eg=01;35:*.gif=01;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;3  
5:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;35:*.pn  
g=01;35:*.svg=01;35:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;3  
5:*.mpg=01;35:*.mpeg=01;35:*.m2v=01;35:*.mkv=01;35:*.webm=01;35:*.o  
gm=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;3  
5:*.nuv=01;35:*.wmv=01;35:*.ASF=01;35:*.rm=01;35:*.rmvb=01;35:*.flc  
=01;35:*.avi=01;35:*.fli=01;35:*.flv=01;35:*.gl=01;35:*.dl=01;35:*.  
xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm=01;35:*.emf=01;35:*.ogv=01;  
35:*.ogx=01;35:*.aac=00;36:*.au=00;36:*.flac=00;36:*.m4a=00;36:*.mi  
d=00;36:*.midi=00;36:*.mka=00;36:*.mp3=00;36:*.mpc=00;36:*.ogg=00;3  
6:*.ra=00;36:*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xsp  
f=00;36:  
XMODIFIERS=@im=ibus  
XDG_SESSION_DESKTOP=ubuntu  
XAUTHORITY=/home/seed/.Xauthority  
XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed  
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh  
SHELL=/bin/bash  
QT_ACCESSIBILITY=1  
GDMSESSION=ubuntu  
LESSCLOSE=/usr/bin/lesspipe %s %s  
GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1  
UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1297  
XDG_VTNR=7  
QT_IM_MODULE=ibus  
PWD=/home/seed/Desktop/LAB1  
JAVA_HOME=/usr/lib/jvm/java-8-oracle  
CLUTTER_IM_MODULE=xim  
ANDROID_HOME=/home/seed/android/android-sdk-linux  
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg  
XDG_DATA_DIRS=/usr/share/ubuntu:/usr/share/gnome:/usr/local/share/:/  
/usr/share/:/var/lib/snapd/desktop  
VTE_VERSION=4205  
JOB=dbus  
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$
```

4.3

## Task 5

### Step 1:

- chown changes the ownership of the setuidenv executable to root
- chmod 4755 sets the write, read and execute permissions, the permissions are then displayed using la -l command

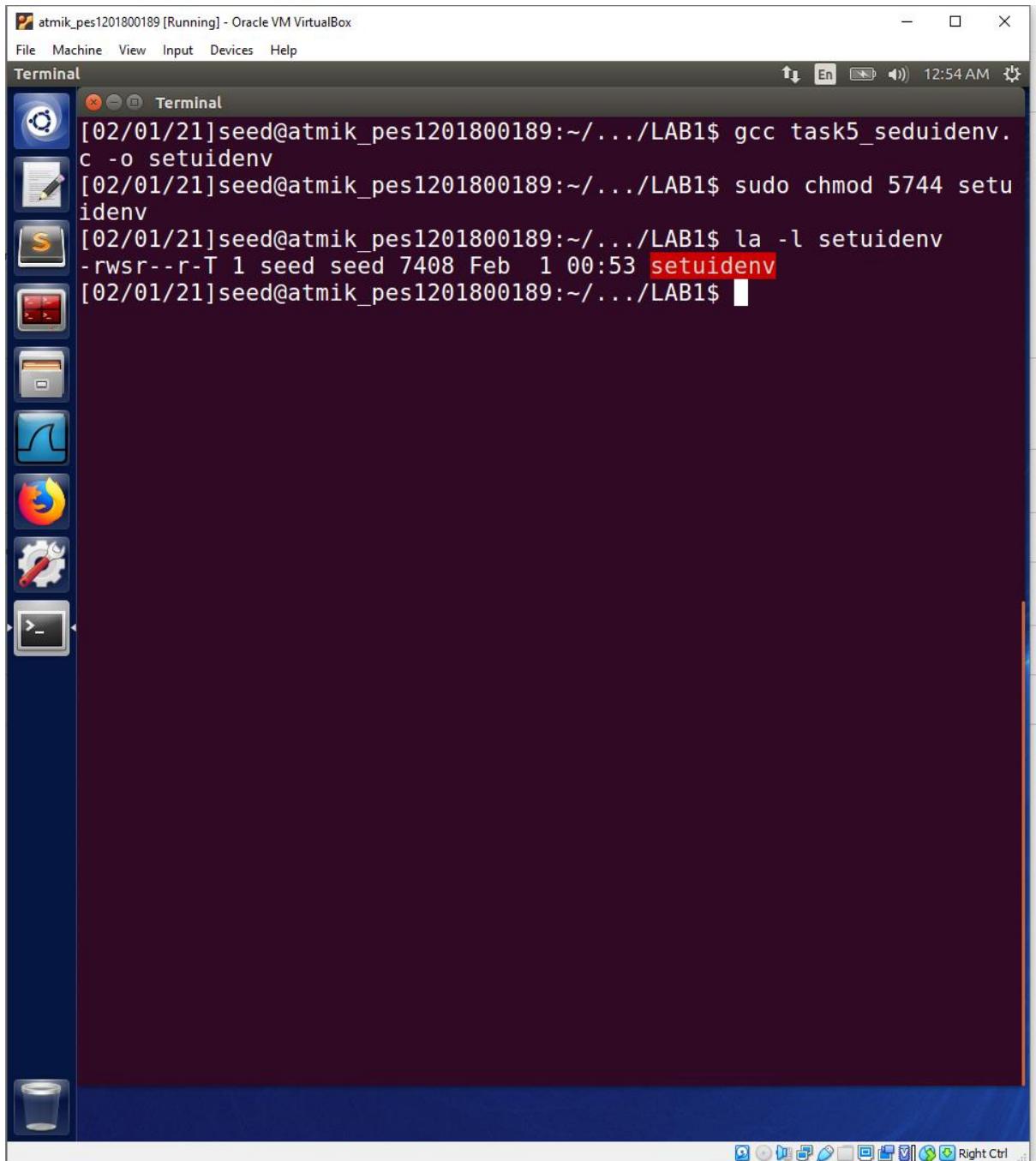


The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "Terminal" and it displays the following command-line session:

```
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ gcc task5_setuidenv.c -o setuidenv
gcc: error: task5_setuidenv.c: No such file or directory
gcc: fatal error: no input files
compilation terminated.
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ gcc task5_setuidenv.c -o setuidenv
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ sudo chown root setuidenv
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ sudo chmod 4755
chmod: missing operand after '4755'
Try 'chmod --help' for more information.
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ chmod 4755 setuidenv
chmod: changing permissions of 'setuidenv': Operation not permitted
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ sudo chmod 4755 setuidenv
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ la -l setuidenv
-rwsr-xr-x 1 root seed 7408 Feb 1 00:50 setuidenv
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$
```

## Step 2:

- chmod 5744 sets the permissions of setuid executable to current working directory which in our case is Desktop/LAB1



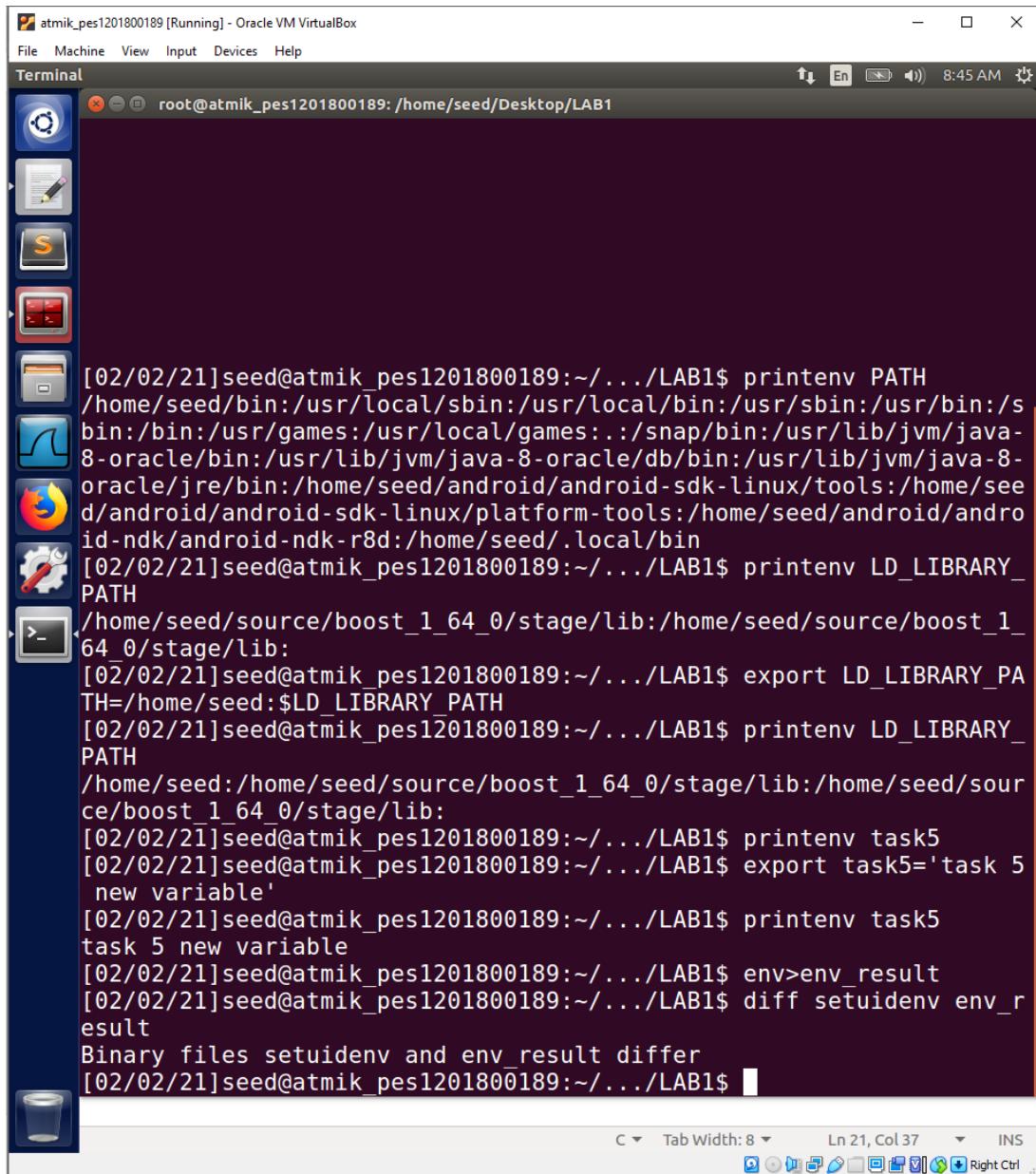
The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "atmik\_pes1201800189 [Running] - Oracle VM VirtualBox". The terminal content shows the following command sequence:

```
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ gcc task5_setuidenv.c -o setuidenv
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ sudo chmod 5744 setuidenv
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ la -l setuidenv
-rwsr--r-T 1 seed seed 7408 Feb 1 00:53 setuidenv
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$
```

The file "setuidenv" is highlighted in red in the terminal output. The desktop interface includes a dock with icons for various applications like a terminal, file manager, and browser, and a taskbar at the bottom.

### Step 3:

- it is observed from the screenshots that all the env variables set in setuidenv are also set in the child process env\_result meaning that the program acquires the values of the environment variables based on the env its running on



The screenshot shows a terminal window titled "atmik\_pes1201800189 [Running] - Oracle VM VirtualBox". The terminal window has a dark background and contains the following text:

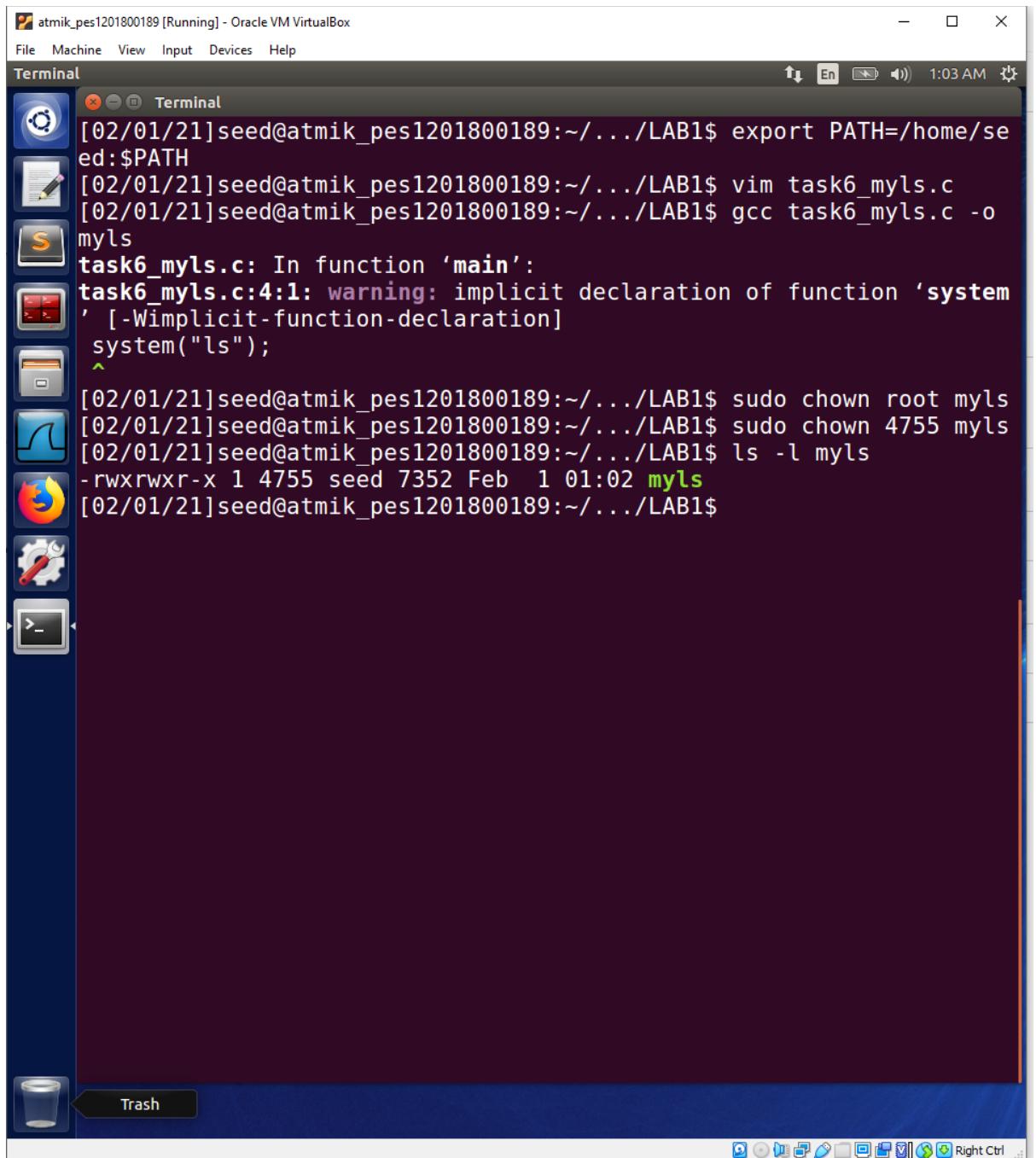
```
[02/02/21]seed@atmik_pes1201800189:~/.../LAB1$ printenv PATH  
/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:./snap/bin:/usr/lib/jvm/java-8-oracle/bin:/usr/lib/jvm/java-8-oracle/db/bin:/usr/lib/jvm/java-8-oracle/jre/bin:/home/seed/android/android-sdk-linux/tools:/home/seed/android/android-ndk/android-ndk-r8d:/home/seed/.local/bin  
[02/02/21]seed@atmik_pes1201800189:~/.../LAB1$ printenv LD_LIBRARY_PATH  
/home/seed/source/boost_1_64_0/stage/lib:/home/seed/source/boost_1_64_0/stage/lib:  
[02/02/21]seed@atmik_pes1201800189:~/.../LAB1$ export LD_LIBRARY_PATH=/home/seed:$LD_LIBRARY_PATH  
[02/02/21]seed@atmik_pes1201800189:~/.../LAB1$ printenv LD_LIBRARY_PATH  
/home/seed:/home/seed/source/boost_1_64_0/stage/lib:/home/seed/source/boost_1_64_0/stage/lib:  
[02/02/21]seed@atmik_pes1201800189:~/.../LAB1$ printenv task5  
[02/02/21]seed@atmik_pes1201800189:~/.../LAB1$ export task5='task 5 new variable'  
[02/02/21]seed@atmik_pes1201800189:~/.../LAB1$ printenv task5  
task 5 new variable  
[02/02/21]seed@atmik_pes1201800189:~/.../LAB1$ env>env_result  
[02/02/21]seed@atmik_pes1201800189:~/.../LAB1$ diff setuidenv env_result  
Binary files setuidenv and env_result differ  
[02/02/21]seed@atmik_pes1201800189:~/.../LAB1$
```

5.3 1

## Task 6

### Step 1:

- Export appends /home/seed to the existing path
- As mentioned before, chown and chmod change ownership to root and permissions of the executable respectively



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "atmik\_pes1201800189 [Running] - Oracle VM VirtualBox". The terminal content shows the following command sequence:

```
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ export PATH=/home/seed:$PATH
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ vim task6_my_ls.c
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ gcc task6_my_ls.c -o myls
task6_my_ls.c: In function 'main':
task6_my_ls.c:4:1: warning: implicit declaration of function 'system'
' [-Wimplicit-function-declaration]
system("ls");
^
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ sudo chown root myls
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ sudo chown 4755 myls
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ ls -l myls
-rwxrwxr-x 1 4755 seed 7352 Feb 1 01:02 myls
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$
```

The desktop interface includes a dock with icons for various applications like a terminal, file manager, and browser, and a taskbar at the bottom.

## Step 2:

- rm /bin/sh and ln -s command will replace /bin/sh with the new z shell located at /bin/zsh to execute new ls program
- ./myls runs the executable from the program which executes the system(ls) function call, the results printed indicate that the command is running in superuser

The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "Terminal" and it displays the following command-line session:

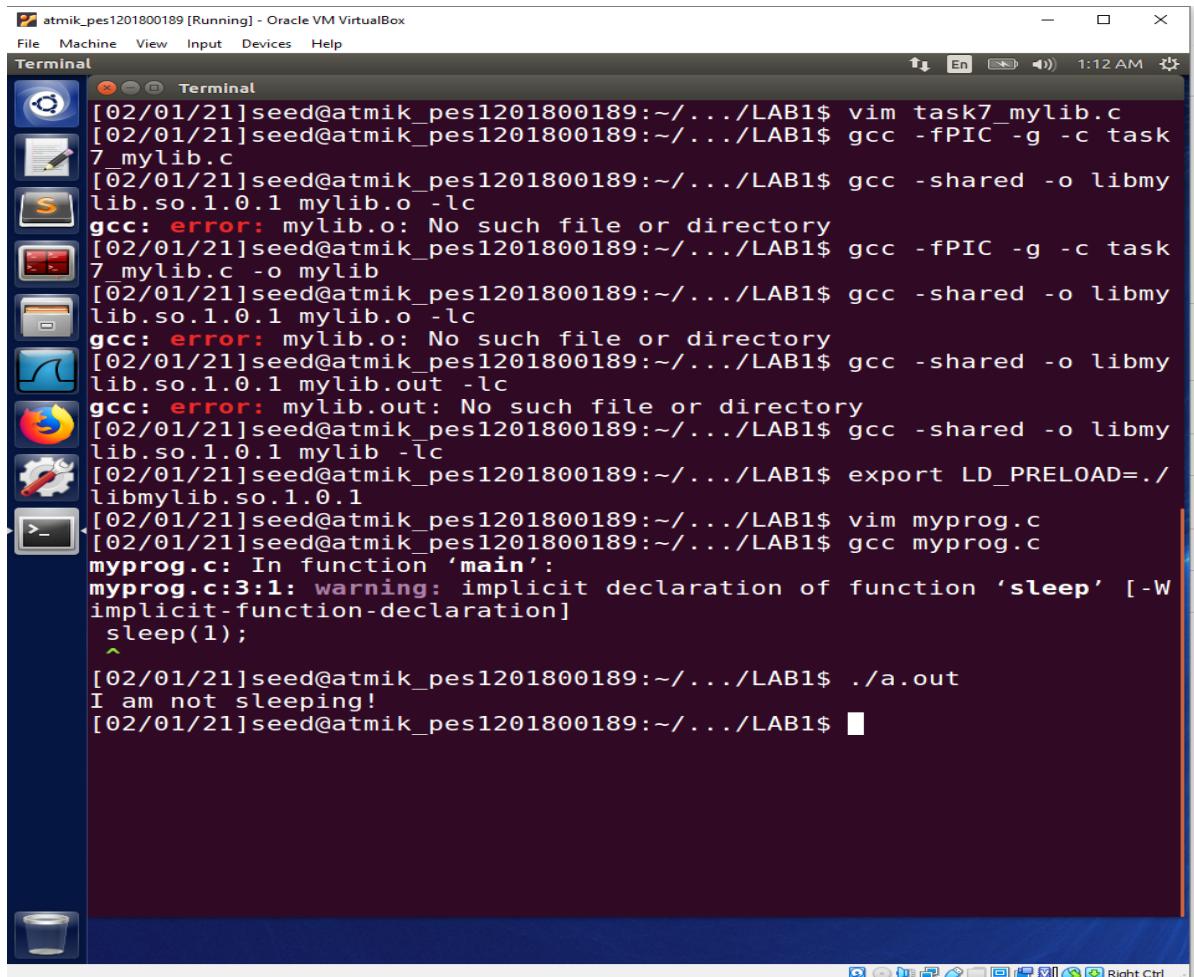
```
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ gcc task6_myls.c -o ls
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ rm /bin/sh
rm: cannot remove '/bin/sh': Permission denied
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ ln -s /bin/zsh /bin/sh
ln: failed to create symbolic link '/bin/sh': File exists
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ sudo rm /bin/sh
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ ln -s /bin/zsh /bin/sh
ln: failed to create symbolic link '/bin/sh': Permission denied
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ sudo ln -s /bin/zsh /bin/sh
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ export PATH=/home/seed/Desktop/Environ_set_uid:$PATH
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ echo $echo
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ echo $PATH
/home/seed/Desktop/Environ_set_uid:/home/seed:/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:./snap/bin:/usr/lib/jvm/java-8-oracle/bin:/usr/lib/jvm/java-8-oracle/db/bin:/usr/lib/jvm/java-8-oracle/jre/bin:/home/seed/android/android-sdk-linux/tools:/home/seed/android/android-sdk-linux/platform-tools:/home/seed/android/android-ndk/android-ndk-r8d:/home/seed/.local/bin
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ ./ls
This is my ls programmy real UID is: 1000
My effective uid: 0
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ ]
```

The terminal window is part of the Oracle VM VirtualBox interface. The desktop environment includes icons for a trash can, a terminal, a file manager, a browser, and other system tools. The taskbar at the bottom shows various application icons.

## Task 7

### Step 1:

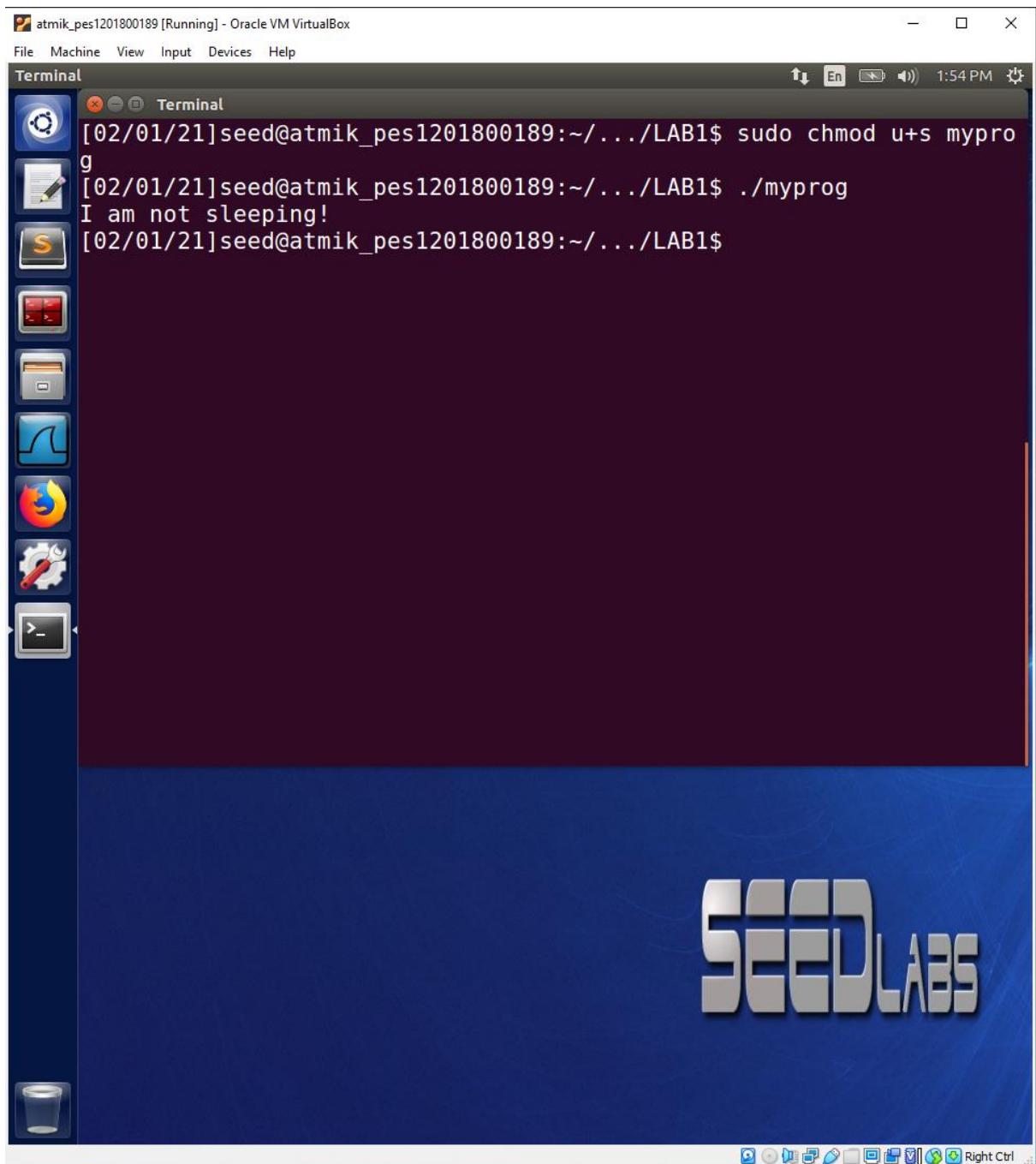
- fPIC option helps in generating position independent code that can be used with shared libraries (which is done in the next command) and would be suitable for dynamic linking (which is better than fpic option as here there is no limit on the global offset table size)
- shared option produces an object which can be linked with other objects to form a executable, in this case libmylib.so.1.0.1 (dynamic lib)
- export LD\_PRELOAD makes the variable point to the dynamic linker/loader created with the -shared step
- we then compile the program in the same directory as the dynamic library libmylib.so.1.0.1 to get required output



```
[02/01/21]seed@atmik_pes1201800189:~/....LAB1$ vim task7_mylib.c
[02/01/21]seed@atmik_pes1201800189:~/....LAB1$ gcc -fPIC -g -c task7_mylib.c
[02/01/21]seed@atmik_pes1201800189:~/....LAB1$ gcc -shared -o libmylib.so.1.0.1 mylib.o -lc
gcc: error: mylib.o: No such file or directory
[02/01/21]seed@atmik_pes1201800189:~/....LAB1$ gcc -fPIC -g -c task7_mylib.c -o mylib
[02/01/21]seed@atmik_pes1201800189:~/....LAB1$ gcc -shared -o libmylib.so.1.0.1 mylib.o -lc
gcc: error: mylib.o: No such file or directory
[02/01/21]seed@atmik_pes1201800189:~/....LAB1$ gcc -shared -o libmylib.so.1.0.1 mylib.out -lc
gcc: error: mylib.out: No such file or directory
[02/01/21]seed@atmik_pes1201800189:~/....LAB1$ gcc -shared -o libmylib.so.1.0.1 mylib -lc
[02/01/21]seed@atmik_pes1201800189:~/....LAB1$ export LD_PRELOAD=../libmylib.so.1.0.1
[02/01/21]seed@atmik_pes1201800189:~/....LAB1$ vim myprog.c
[02/01/21]seed@atmik_pes1201800189:~/....LAB1$ gcc myprog.c
myprog.c: In function `main':
myprog.c:3:1: warning: implicit declaration of function `sleep' [-Wimplicit-function-declaration]
 sleep(1);
 ^
[02/01/21]seed@atmik_pes1201800189:~/....LAB1$ ./a.out
I am not sleeping!
[02/01/21]seed@atmik_pes1201800189:~/....LAB1$ █
```

## Step 2:

- we execute under 4 different behaviours here, the way we initialise these behaviours/configurations is detailed in the previous tasks
  - o run myprog as regular user
    - LD\_PRELOAD loads the function defined in the libmylib.so.1.0.1 into RAM from main memory and executed the function defined in c file which would be library for sleep func.
  - o make myprog a setuid root program and run as normal user
    - LD\_PRELOAD has the value ./libmylib.so.1.0.1 as the program is running in the environment that it was created in. hence we know that environment variables will be the same for everything running in /Desktop/LAB1. This will then execute similar to first configuration with the UID of the owner and not current user.
  - o make myprog a setuid root program, export the LD\_PRELOAD environment variable in root once again and run
    - since we are in a different environment (root user) hence we need to export LD\_PRELOAD again as it isn't defined here. Once we do that we can execute the program and it will work as before
  - o make it set uid user1 program and run as non root user
    - the permissions are assigned only to user1 and since the /Desktop/LAB1 is the superuser , it could access myprog and LD\_PRELOAD loaded and hence run the executable.



7.2.1

atmik\_pes1201800189 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal

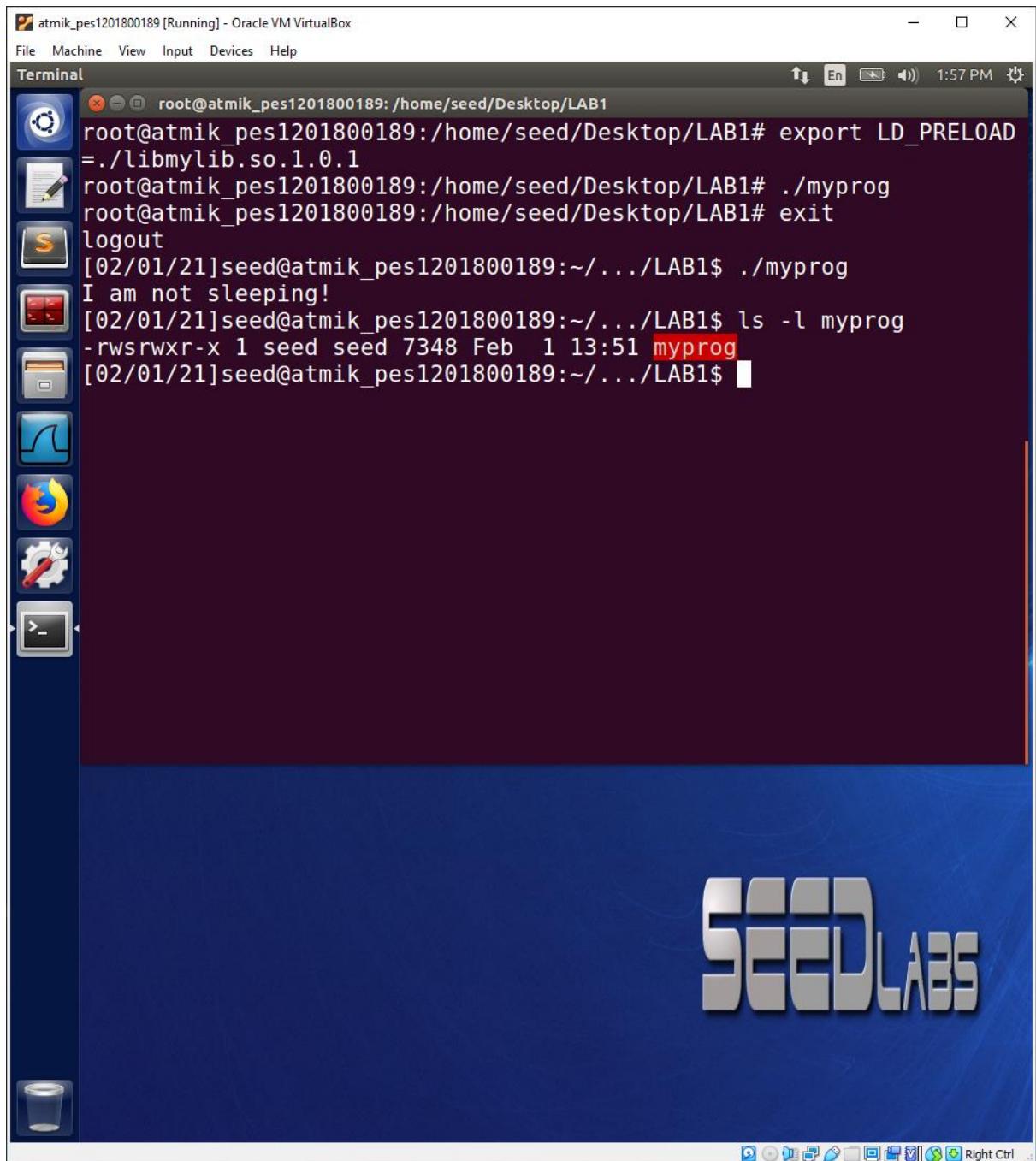
```
root@atmik_pes1201800189:/home/seed/Desktop/LAB1
--extrausers           Use the extra users database

root@atmik_pes1201800189:/home/seed# clear

root@atmik_pes1201800189:/home/seed# useradd -d /usr/user1 -m user1
useradd: user 'user1' already exists
root@atmik_pes1201800189:/home/seed# cd Desktop
root@atmik_pes1201800189:/home/seed/Desktop# cd LAB1
root@atmik_pes1201800189:/home/seed/Desktop/LAB1# useradd -d /usr/u
ser1 -m user1
useradd: user 'user1' already exists
root@atmik_pes1201800189:/home/seed/Desktop/LAB1# chown user1 mypro
g
root@atmik_pes1201800189:/home/seed/Desktop/LAB1# chgrp user1 mypro
g
root@atmik_pes1201800189:/home/seed/Desktop/LAB1# exit
logout
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ export LD_PRELOAD=.
/libmylib.so.1.0.1
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ ./myprog
I am not sleeping!
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ ls -l myprog
-rwxrwxr-x 1 user1 user1 7348 Feb  1 13:51 myprog
```

SEEDLABS

7.2.2



7.2.3

### Step 3:

- The below screenshots enforce the reasonings for the above mentioned behaviours in step 2. We see that child processes don't necessarily inherit environment variables LD\_PRELOAD)

```
atmik_pes1201800189 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
root@atmik_pes1201800189:/home/seed/Desktop/LAB1# gcc myprog.c -o myprog
myprog.c: In function 'main':
myprog.c:3:1: warning: implicit declaration of function 'sleep' [-Wimplicit-function-declaration]
    sleep(1);
^
root@atmik_pes1201800189:/home/seed/Desktop/LAB1# chmod 4755 myprog
chmod: cannot access 'mypro': No such file or directory
root@atmik_pes1201800189:/home/seed/Desktop/LAB1# chmod 4755 myprg
chmod: cannot access 'myprg': No such file or directory
root@atmik_pes1201800189:/home/seed/Desktop/LAB1# chmod 4755 myprog
root@atmik_pes1201800189:/home/seed/Desktop/LAB1# ls -l myprog
-rwsr-xr-x 1 root root 7348 Feb 1 14:03 myprog
root@atmik_pes1201800189:/home/seed/Desktop/LAB1# export LD_PRELOAD=../libmylib.so.1.0.1
root@atmik_pes1201800189:/home/seed/Desktop/LAB1# ls -l myprog
-rwsr-xr-x 1 root root 7348 Feb 1 14:03 myprog
root@atmik_pes1201800189:/home/seed/Desktop/LAB1# export LD_PRELOAD=../libmylib.so.1.0.1
root@atmik_pes1201800189:/home/seed/Desktop/LAB1# exit
```

atmik\_pes1201800189 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal

```
root@atmik_pes1201800189:/home/seed/Desktop/LAB1
root@atmik_pes1201800189:/home/seed/Desktop/LAB1# chmod 4755 mypro
chmod: cannot access 'mypro': No such file or directory
root@atmik_pes1201800189:/home/seed/Desktop/LAB1# chmod 4755 myprg
chmod: cannot access 'myprg': No such file or directory
root@atmik_pes1201800189:/home/seed/Desktop/LAB1# chmod 4755 myprog
root@atmik_pes1201800189:/home/seed/Desktop/LAB1# ls -l myprog
-rwsr-xr-x 1 root root 7348 Feb 1 14:03 myprog
root@atmik_pes1201800189:/home/seed/Desktop/LAB1# export LD_PRELOAD=./libmylib.so.1.0.1
root@atmik_pes1201800189:/home/seed/Desktop/LAB1# ls -l myprog
-rwsr-xr-x 1 root root 7348 Feb 1 14:03 myprog
root@atmik_pes1201800189:/home/seed/Desktop/LAB1# export LD_PRELOAD=./libmylib.so.1.0.1
root@atmik_pes1201800189:/home/seed/Desktop/LAB1# exit
logout
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ ls -l myprog
-rwsr-xr-x 1 root root 7348 Feb 1 14:03 myprog
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ export LD_PRELOAD=./libmylib.so.1.0.1
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ whoami
seed
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ ./myprog
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ █
```

SEEDLABS

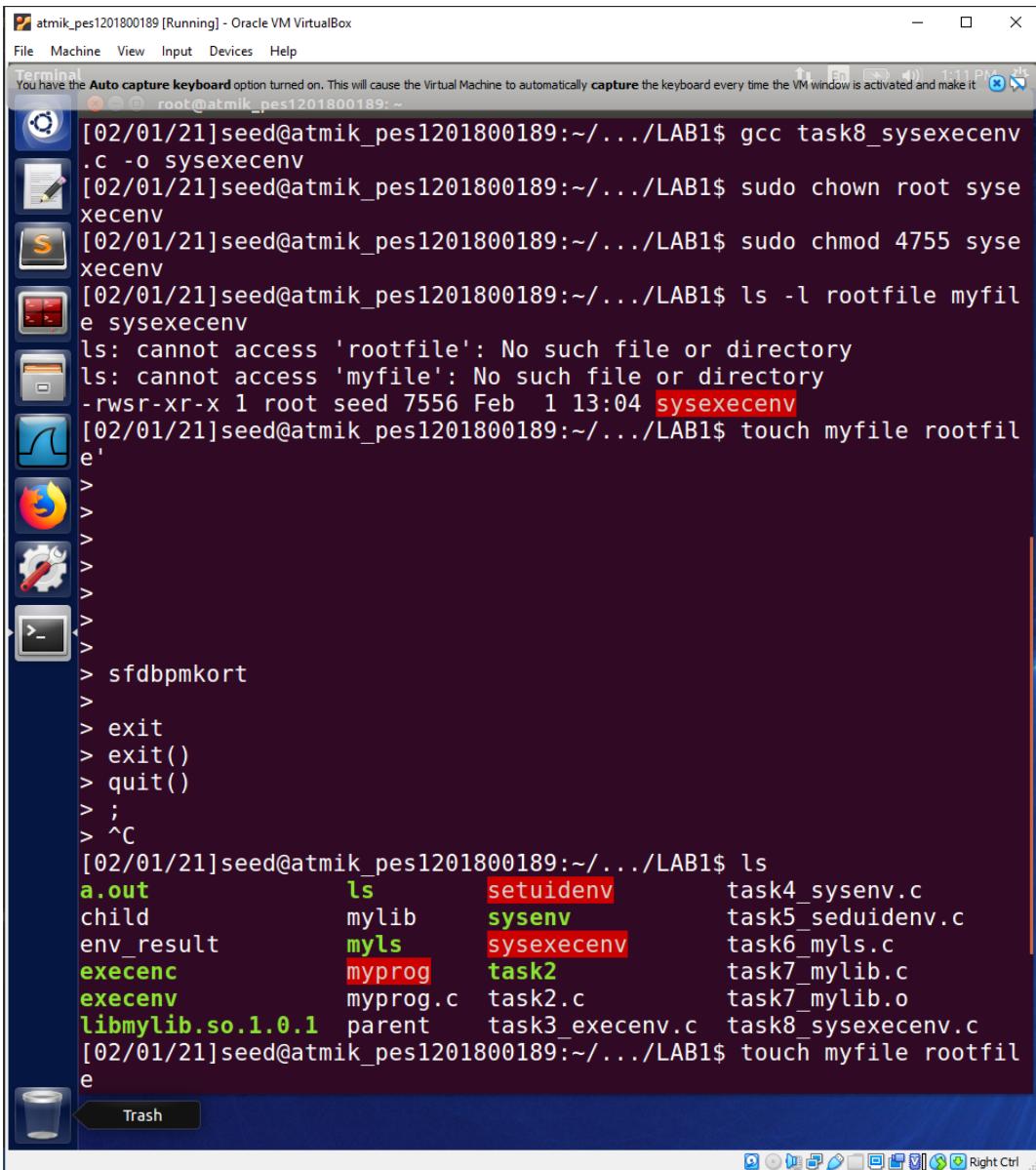
7.3.2

## Task 8

### Step 1:

- System() makes the /bin/cal file execute which inturn displays contents of myfile
- It also invokes the shell with root privileges as we are able to delete rootfile using rm rootfile which we wouldn't have been able to do if we didn't have those root privileges that system helps invoke

8.1 1



The screenshot shows a terminal window titled "atmik\_pes1201800189 [Running] - Oracle VM VirtualBox". The terminal session is as follows:

```
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ gcc task8_sysexecenv.c -o sysexecenv
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ sudo chown root sysexecenv
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ sudo chmod 4755 sysexecenv
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ ls -l rootfile myfile sysexecenv
ls: cannot access 'rootfile': No such file or directory
ls: cannot access 'myfile': No such file or directory
-rwsr-xr-x 1 root seed 7556 Feb 1 13:04 sysexecenv
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ touch myfile rootfile
>
>
>
>
>
> sfdbpmkort
>
> exit
> exit()
> quit()
> ;
> ^C
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ ls
a.out      ls      setuidenv      task4_sysenv.c
child      mylib   sysenv        task5_seduidenv.c
env_result myls    sysexecenv   task6_myls.c
execenc   myprog  task2         task7_mylib.c
execenv   myprog.c task2.c      task7_mylib.o
libmylib.so.1.0.1 parent  task3_execenv.c task8_sysexecenv.c
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ touch myfile rootfile
```

The terminal window has a dark blue background and a light blue header bar. The command line is white, and the output text is white. The file names "rootfile" and "myfile" are highlighted in red, while other file names like "a.out", "ls", "setuidenv", etc., are in green. The "sysexecenv" file is shown with its full path and permissions: -rwsr-xr-x 1 root seed 7556 Feb 1 13:04 sysexecenv.

atmik\_pes1201800189 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal

You have the Auto capture keyboard option turned on. This will cause the Virtual Machine to automatically capture the keyboard every time the VM window is activated and make it available to the guest OS.

```
e'
>
>
>
>
> sfdbpmkort
>
> exit()
> quit()
> ;
> ^C
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ ls
a.out          ls      setuidenv    task4_sysenv.c
child         mylib   sysenv       task5_seduidenv.c
env_result    myls    sysexecenv  task6_myls.c
execenc       myprog  task2        task7_mylib.c
execenv       myprog.c task2.c     task7_mylib.o
libmylib.so.1.0.1 parent  task3_execenv.c task8_sysexecenv.c
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ touch myfile rootfile
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ sudo chown root root
file
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ ls -l rootfile myfile
sysexecenv
-rw-rw-r-- 1 seed seed    0 Feb  1 13:09 myfile
-rw-rw-r-- 1 root seed    0 Feb  1 13:09 rootfile
-rwsr-xr-x 1 root seed 7556 Feb  1 13:04 sysexecenv
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ ./sysexecenv "myfile"
;rm rootfile"
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$ ls -l rootfile
-rw-rw-r-- 1 root seed    0 Feb  1 13:09 rootfile
[02/01/21]seed@atmik_pes1201800189:~/.../LAB1$
```

8.1.2

## Step 2:

- Execve() doesn't invoke shell with root privileges and executes the /bin/cat executable which displays myfile and rootfile
- When we try to give same command as before now, it doesn't work as it is executed as /bin/cat 'myfile;rm rootfile' and not separately as before(/bin/cat myfile; rm rootfile)
- Hence this doesn't delete the rootfile and nothing happens , making it a safer option

The screenshot shows a terminal window titled "atmik\_pes1201800189 [Running] - Oracle VM VirtualBox". The terminal session is as follows:

```
root@atmik_pes1201800189:~/.LAB1$ vim task8_sysexecenv
.c
[02/01/21]seed@atmik_pes1201800189:~/.LAB1$ gcc task8_sysexecenv
.c -o sysexecenv
task8_sysexecenv.c: In function 'main':
task8_sysexecenv.c:19:1: warning: implicit declaration of function
'execve' [-Wimplicit-function-declaration]
execve(v[0], v,NULL);
^
[02/01/21]seed@atmik_pes1201800189:~/.LAB1$ sudo chown root sysexecenv
[02/01/21]seed@atmik_pes1201800189:~/.LAB1$ sudo chmod 4755 sysexecenv
[02/01/21]seed@atmik_pes1201800189:~/.LAB1$ ls -l rootfile myfile sysexecenv
-rw-rw-r-- 1 seed seed    0 Feb  1 13:09 myfile
-rw-rw-r-- 1 root seed    0 Feb  1 13:09 rootfile
-rwsr-xr-x 1 root seed 7556 Feb  1 13:13 sysexecenv
[02/01/21]seed@atmik_pes1201800189:~/.LAB1$ ./sysexecenv "myfile"
;rm rootfile"
/bin/cat: 'myfile;rm rootfile': No such file or directory
[02/01/21]seed@atmik_pes1201800189:~/.LAB1$ ls -l rootfile
-rw-rw-r-- 1 root seed 0 Feb  1 13:09 rootfile
[02/01/21]seed@atmik_pes1201800189:~/.LAB1$
```

## Task 9

- Please note,I have changed permissions and executed the chown and chmod command before clearing, I cleared terminal screen by accident.
- We are able to modify cat/zzz through ./capleak and not manually as only capleak has root privileges and not us. Hence this enforces the principle of least privilege.

```
atmik_pes1201800189 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal Terminal File Edit View Search Terminal Help
root@atmik_pes1201800189: /home/seed/Desktop/LAB1
[02/02/21]seed@atmik_pes1201800189:~/.../LAB1$ sudo chown root capleak
[02/02/21]seed@atmik_pes1201800189:~/.../LAB1$ sudo chmod 4755 capleak
[02/02/21]seed@atmik_pes1201800189:~/.../LAB1$ ls -l capleak
-rwsr-xr-x 1 root seed 7648 Feb 2 09:07 capleak
[02/02/21]seed@atmik_pes1201800189:~/.../LAB1$ touch /etc/zzz
touch: cannot touch '/etc/zzz': Permission denied
[02/02/21]seed@atmik_pes1201800189:~/.../LAB1$ cat /etc/zzz
cat: /etc/zzz: No such file or directory
[02/02/21]seed@atmik_pes1201800189:~/.../LAB1$ ./capleak
Cannot open/etc/zzz
[02/02/21]seed@atmik_pes1201800189:~/.../LAB1$ sudo touch /etc/zzz
[02/02/21]seed@atmik_pes1201800189:~/.../LAB1$ ./capleak
[02/02/21]seed@atmik_pes1201800189:~/.../LAB1$ cat /etc/zzz
MaliciousData
[02/02/21]seed@atmik_pes1201800189:~/.../LAB1$
```