

# **INFORMATION SECURITY LABORATORY**

## **WEEK 1**

**BY: RAJDEEP SENGUPTA**

**SRN: PES1201800144**

**SECTION: C**

Note: Please find the terminal username as my SRN followed by my name 'seed@pes1201800144rajdeep'. Also find the screenshots followed by observations for each task.

## Screenshots Task 1:

The image shows a Linux desktop environment. On the left is a vertical dock with icons for a terminal, file manager, web browser, and other applications. The main window is a terminal titled "Terminal" with the following text:

```
seed@pes1201800144rajdeep:~$printenv PWD
/home/seed
seed@pes1201800144rajdeep:~$env |grep PWD
PWD=/home/seed
seed@pes1201800144rajdeep:~$
```

The desktop background features a dark blue-grey gradient with a large, light-colored spiral pattern in the center. The top of the screen has a system tray with icons for network, volume, and battery, along with the time "2:35 AM".The screenshot displays the Kali Linux desktop interface. On the left side, there is a vertical dock containing several application icons: a network icon at the top, followed by file manager, Firefox web browser, LibreOffice suite, and a terminal icon at the bottom. The main area of the screen features a dark blue background with a faint, artistic spiral pattern. A terminal window titled "Terminal" is open in the center-left portion of the screen. It contains a series of shell commands and their outputs, demonstrating the export, unset, and printenv operations. The system status bar at the very top shows the language set to English, battery level, signal strength, and the time as 2:36 AM.

**Terminal**

```
seed@pes1201800144rajdeep:~$export foo='test string Rajdeep PES1201800144'
seed@pes1201800144rajdeep:~$printenv foo
test string Rajdeep PES1201800144
seed@pes1201800144rajdeep:~$
seed@pes1201800144rajdeep:~$
seed@pes1201800144rajdeep:~$
seed@pes1201800144rajdeep:~$
seed@pes1201800144rajdeep:~$
seed@pes1201800144rajdeep:~$
seed@pes1201800144rajdeep:~$
seed@pes1201800144rajdeep:~$
seed@pes1201800144rajdeep:~$
seed@pes1201800144rajdeep:~$unset foo
seed@pes1201800144rajdeep:~$printenv foo
seed@pes1201800144rajdeep:~$
```

## Observation Task 1::

printenv prints out the value of the environment variable

export command is used to set environment variables

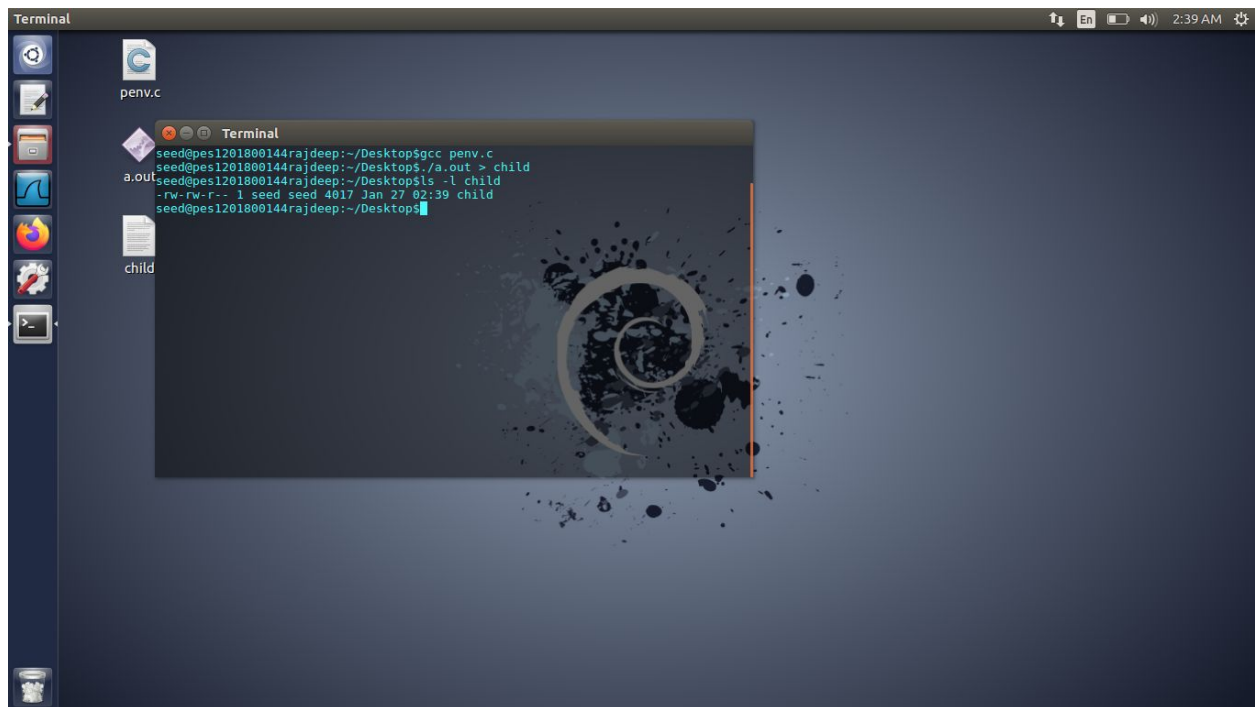
unset command is used to unset environment variables

**Using export and unset commands makes temporary environment variables which are unset when the system is rebooted. Whereas if the changes are directly made to the .bashrc file, then the changes stay permanently even after reboot.**

=====

## TASK 2: Inheriting environment variables from parents

### Screenshots Task 2:



The screenshot shows a Linux desktop environment with a terminal window open. The terminal displays the following commands and output:

```
seed@pes1201800144rajdeep:~/Desktop$ gcc penv.c
seed@pes1201800144rajdeep:~/Desktop$ ./a.out > child
seed@pes1201800144rajdeep:~/Desktop$ ls -l child
-rw-rw-r-- 1 seed seed 4617 Jan 27 02:39 child
seed@pes1201800144rajdeep:~/Desktop$
```

The terminal window is titled "Terminal" and shows the user "seed" at the host "pes1201800144rajdeep". The desktop background features a dark blue and black abstract design with a white spiral. The terminal window is positioned over a desktop with icons for "penv.c", "a.out", and "child".

Permissions of child output

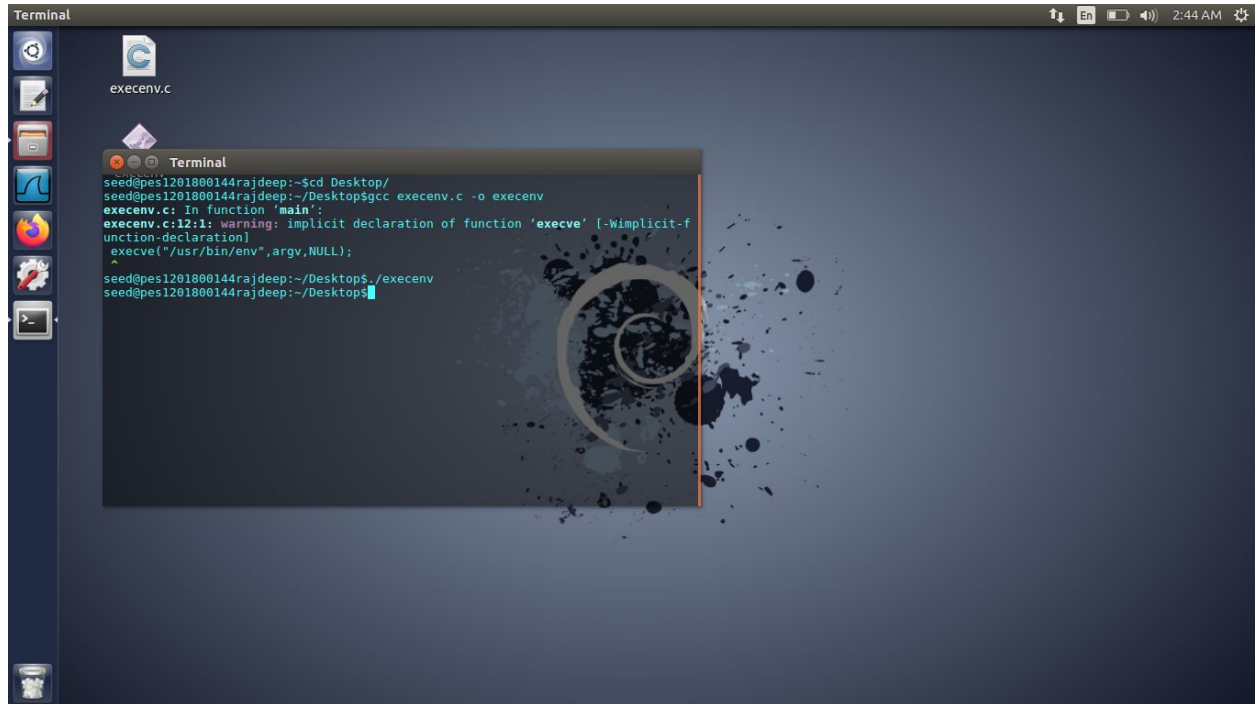


## Observation Task 2:

There will not be any difference between parent and child programs

**All the environment variables of the parent are inherited to the child for any process.**

## TASK 3: Environment variables and execve()



```
Terminal
seed@pes1201800144rajdeep:~/Desktop$ gcc execenv.c -o execenv
execenv.c: In function 'main':
execenv.c:12:11: warning: implicit declaration of function 'execve' [-Wimplicit-f
function-declaration]
execve("/usr/bin/env",argv,NULL);
^
seed@pes1201800144rajdeep:~/Desktop$ ./execenv
seed@pes1201800144rajdeep:~/Desktop$
```

Output on executing code with 'execve("/usr/bin/env", arg, NULL)'

```
Terminal
seed@pes1201800144rajdeep:~/Desktop$. ./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=4285
XDG_MENU_PREFIX=gnome-
SHELL=/bin/bash
DERBY_HOME=/usr/lib/jvm/java-8-oracle/db
QT_LINUX_ACCESSIBILITY_ALWAYS_ON=1
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
WINDOWID=33554442
UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1311
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:cd=40;33:or=01;31: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:*.lzh=01;31:*.lzm=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7z=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:*.mpg=01;35:*.mpeg=01;35:*.m2v=01;35:*.mkv=01;35:*.webm=01;35:*.ogm=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.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:*.mid=00;36:*.midi=00;36:*.mka=00;36:*.mp3=00;36:*.mpc=00;36:*.ogg=00;36:*.ra=00;36:*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:
QT_ACCESSIBILITY=1
LD_LIBRARY_PATH=/home/seed/source/boost_1_64_0/stage/lib:/home/seed/source/boost_1_64_0/stage/lib:
XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0
XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
DEFAULTS_PATH=/usr/share/gconf/ubuntu.defaults
SESSION_MANAGER=local/VM:0/tmp/.ICE-unix/1701,unix/VM:/tmp/.ICE-unix/1701
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg
DESKTOP_SESSION=ubuntu
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-sdk-linux/platform-tools:/home/seed/android/android-ndk-r8d:/home/seed/.local/bin
QT_IM_MODULE=ibus
QT_OPA_PLATFORMTHEME=appmenu-qt5
XDG_SESSION_TYPE=x11
PWD=/home/seed/Desktop
JOB=dbus
XMODIFIERS=@im=ibus
JAVA_HOME=/usr/lib/jvm/java-8-oracle
```

Output on executing code with 'execve("/usr/bin/env", arg, environ)'

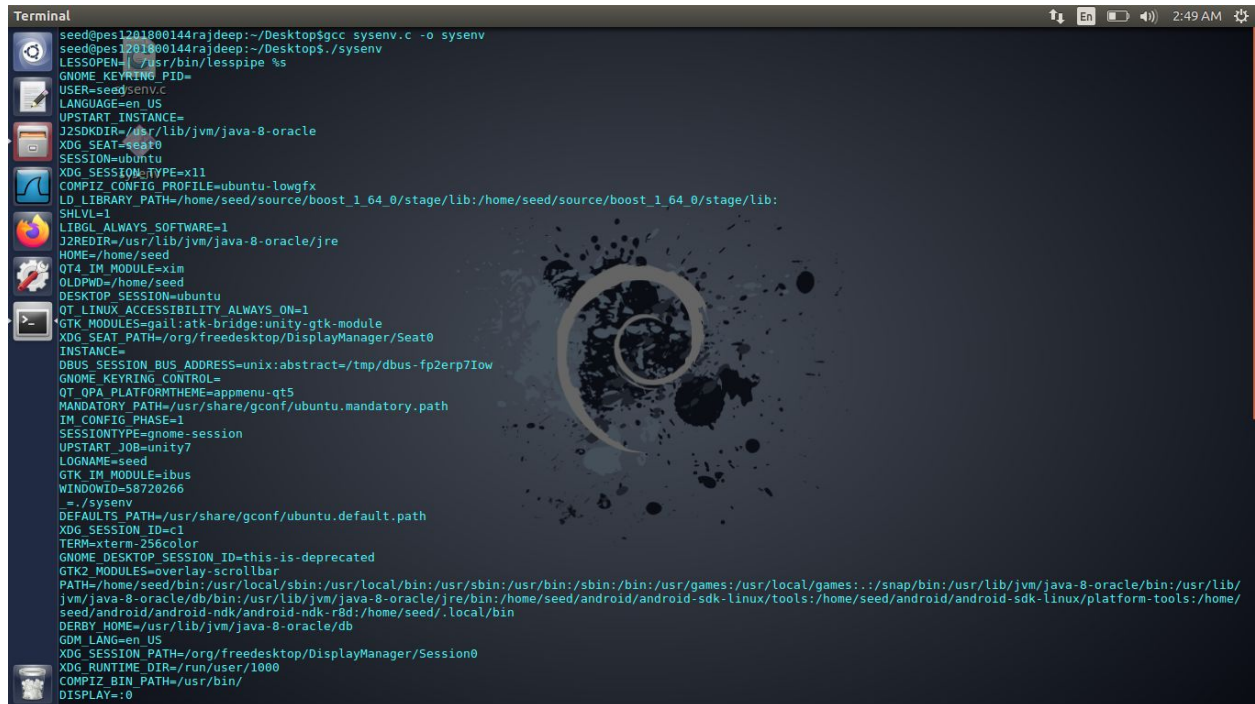
### Observation Task 3:

- When execve(, , NULL) is called, environment variables are not inherited as seen in first screenshot
  - When execve(, , environ) is called, environment variables are passed to the new program and when the new program is executed, all the environment variables can be seen in the second screenshot
- execve() replaces the code and data of the current process by code and data loaded from an executable file.**

=====



## TASK 4: Environment variables and system() Screenshots Task 4:

A terminal window titled 'Terminal' showing the execution of a C program. The program prints a list of environment variables and then calls system(). The output of system() is a shell prompt followed by the same list of environment variables. The background of the terminal window features a dark blue and black abstract pattern with a white spiral. The terminal output is as follows:

```
seed@pes1201800144rajdeep:~/Desktop$ gcc sysenv.c -o sysenv
seed@pes1201800144rajdeep:~/Desktop$ ./sysenv
LESSOPEN=| /usr/bin/lesspipe %s
GNOME_KEYRING_PID=
USER=seed
LANG=en_US
UPSTART_INSTANCE=
J2SDKDIR=/usr/lib/jvm/java-8-oracle
XDG_SEAT=seat0
SESSION=ubuntu
XDG_SESSION_TYPE=x11
COMPIZ_CONFIG_PROFILE=ubuntu-lowfx
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_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-fp2erp7Iow
GNOME_KEYRING_CONTROL=
QT_QPA_PLATFORMTHEME=appmenu-gt5
MANDATORY_PATH=/usr/share/gconf/ubuntu.mandatory.path
IM_CONFIG_PHASE=1
SESSIONTYPE=gnome-session
UPSTART_JOB=unity7
LOGNAME=seed
GTK_IM_MODULE=ibus
WINDOWID=58720266
./sysenv
DEFAULTS_PATH=/usr/share/gconf/ubuntu.default.path
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/sbin:/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-ndk-linux/tools:/home/seed/android-sdk-linux/platform-tools:/home/
seed/android/android-ndk/android-ndk-r8d:/home/seed/.local/bin
DERBY_HOME=/usr/lib/jvm/java-8-oracle/db
GDM_LANG=en_US
XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0
XDG_RUNTIME_DIR=/run/user/1000
COMPIZ_BIN_PATH=/usr/bin/
DISPLAY=:0
```

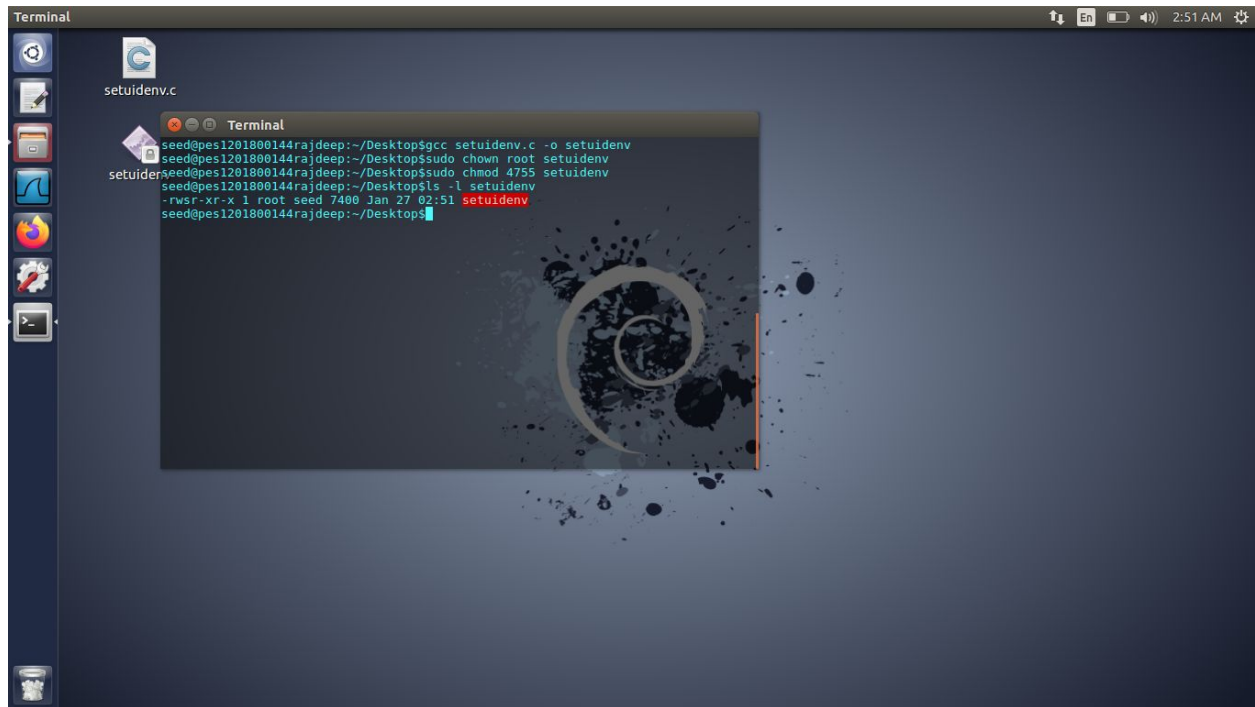
Execution using system() call. So the environment variables of calling process is passed to new program /bin/sh

## Observation Task 4:

system() call inherits the environment variables as we can see in the screenshot.  
system() calls execl() which further calls execve(). Hence all the environment variables are passed to the new program like execve() call.

=====

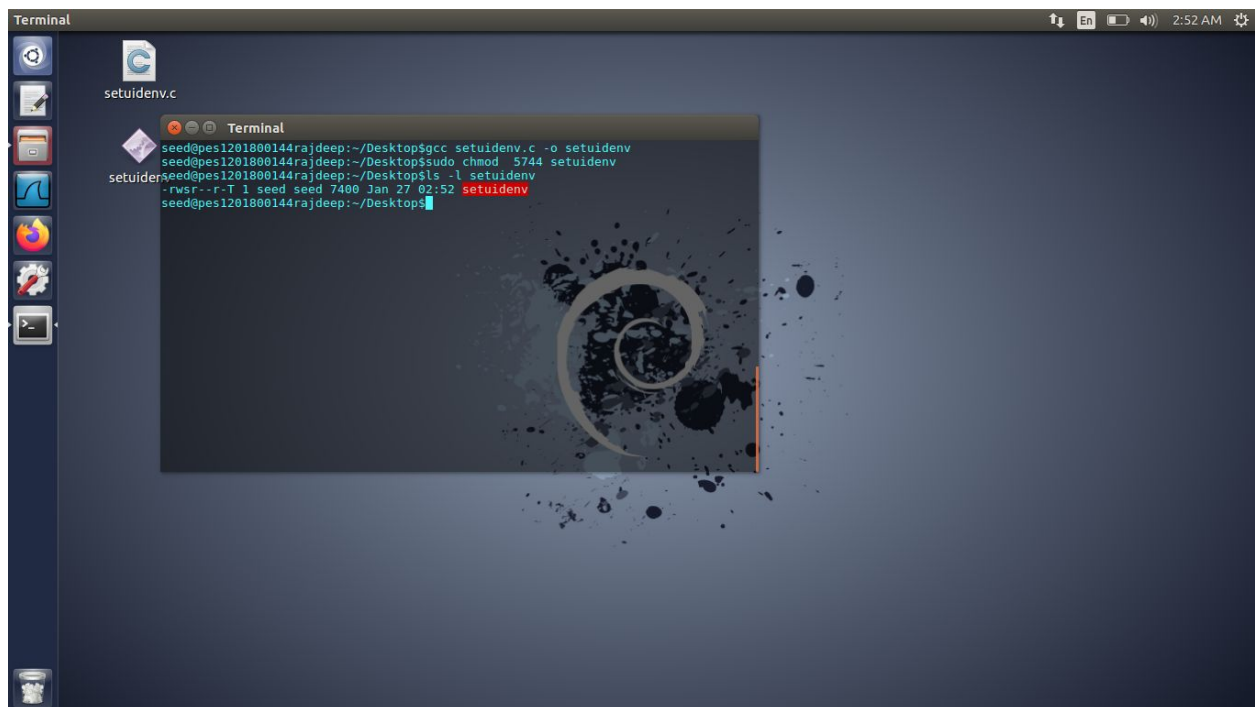
## TASK 5: Environment variable and Set-UID programs



The image shows a terminal window with a dark background and a spiral graphic. The terminal output is as follows:

```
seed@pes1201800144rajdeep:~/Desktop$ gcc setuidenv.c -o setuidenv
seed@pes1201800144rajdeep:~/Desktop$ sudo chown root setuidenv
setuidenv$ sudo chmod 4755 setuidenv
seed@pes1201800144rajdeep:~/Desktop$ ls -l setuidenv
-rwsr-xr-x 1 root seed 7400 Jan 27 02:51 setuidenv
seed@pes1201800144rajdeep:~/Desktop$
```

Making the code owner as root using chmod and chown



The image shows a terminal window with a dark background and a spiral graphic. The terminal output is as follows:

```
seed@pes1201800144rajdeep:~/Desktop$ gcc setuidenv.c -o setuidenv
seed@pes1201800144rajdeep:~/Desktop$ sudo chown 5744 setuidenv
setuidenv$ sudo chmod 5744 setuidenv
seed@pes1201800144rajdeep:~/Desktop$ ls -l setuidenv
-rwsr--r-T 1 seed seed 7400 Jan 27 02:52 setuidenv
seed@pes1201800144rajdeep:~/Desktop$
```

Changing owner to root and making it Set-UID program using chmod 5744



```
Terminal
setuidenv.c

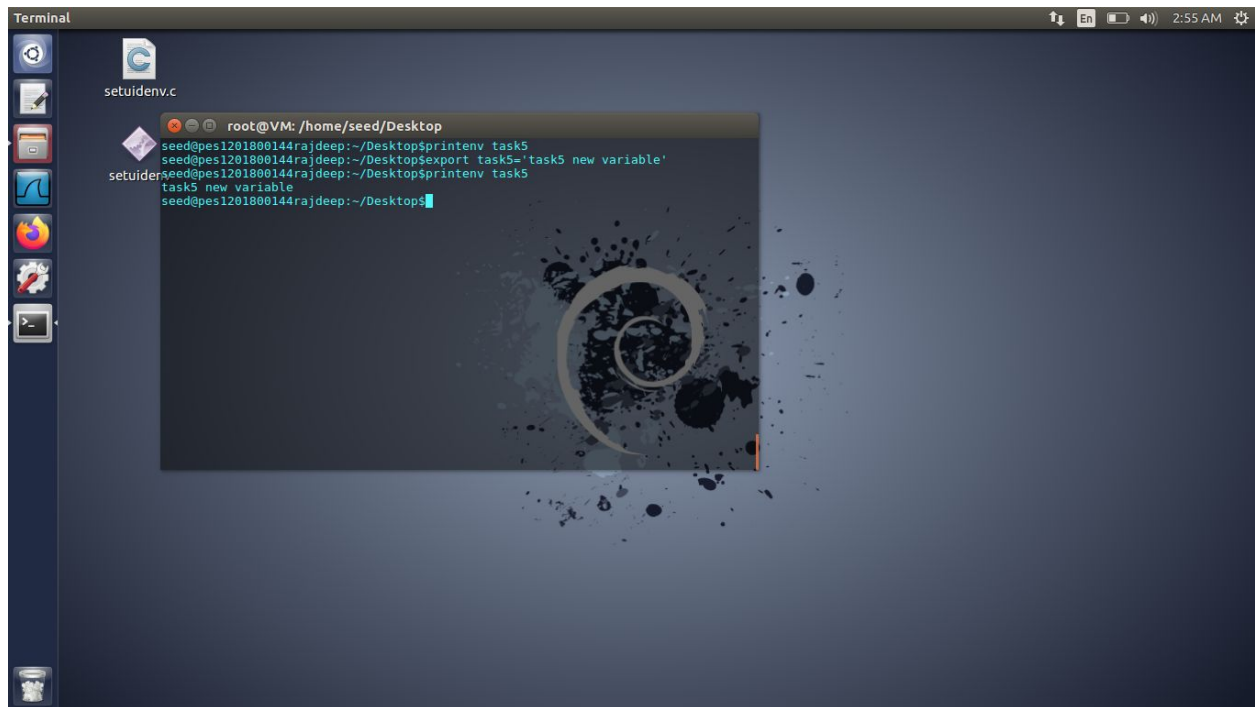
root@VM: /home/seed/Desktop
seed@pes1201800144rajdeep: ~/Desktop$ printenv PATH
/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin:/usr/lib/jvm/java-8-oracle/bin:/usr/lib/jvm/java-8-oracle/db/bin:/usr/lib/jvm/java-8-oracle/jre/bin:/home/seed/android/android-sdk-linux/tools:/home/seed/android/android-sdk-linux/platform-tools:/home/seed/android/android-ndk/android-ndk-r8d:/home/seed/.local/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
seed@pes1201800144rajdeep: ~/Desktop$
```

Output of 'printenv PATH'

```
Terminal
setuidenv.c

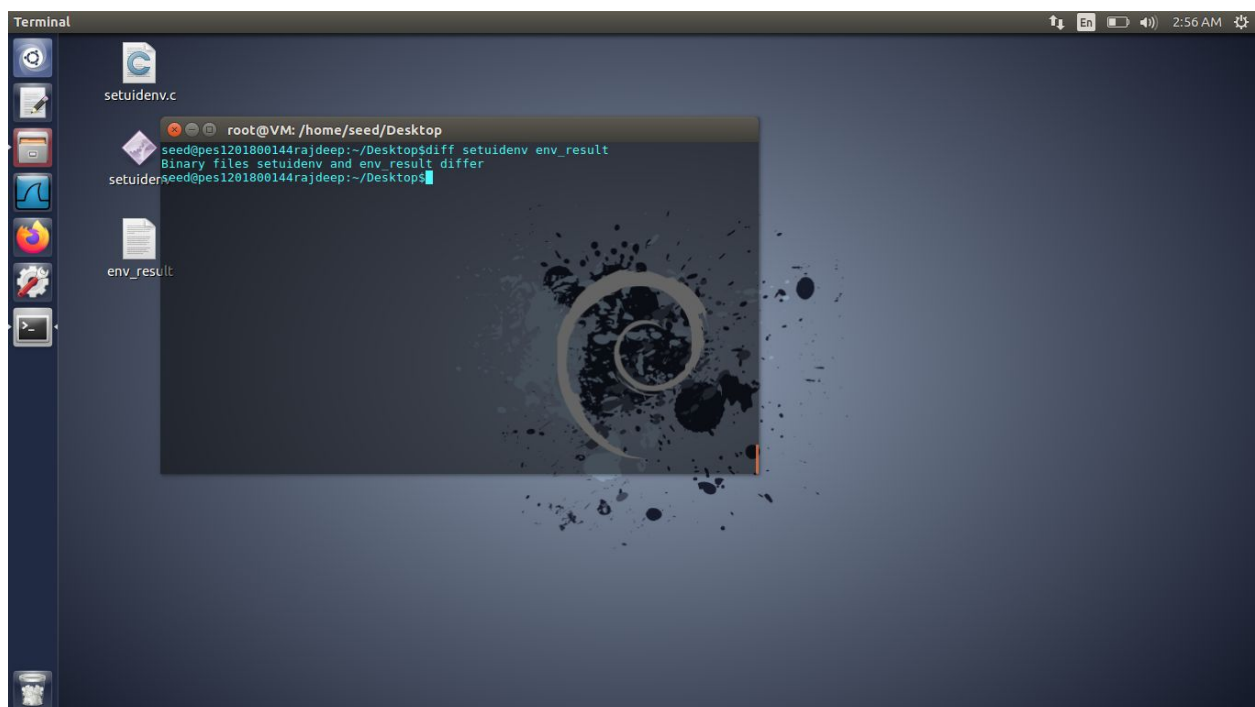
root@VM: /home/seed/Desktop
seed@pes1201800144rajdeep: ~/Desktop$ export LD_LIBRARY_PATH=/home/seed:$LD_LIBRARY_PATH
seed@pes1201800144rajdeep: ~/Desktop$ printenv LD_LIBRARY_PATH
/home/seed:/home/seed/source/boost_1_64_0/stage/lib:/home/seed/source/boost_1_64_0/stage/lib:
seed@pes1201800144rajdeep: ~/Desktop$
```

Setting LD\_LIBRARY\_PATH to /home/seed:\$LD\_LIBRARY\_PATH

A terminal window titled 'Terminal' with a dark background and a vertical sidebar of application icons on the left. The terminal shows a user 'root' at a VM with the path '/home/seed/Desktop'. The user runs a series of commands: 'setuidenv.c', 'printenv task5', 'export task5='task5 new variable'', and 'printenv task5'. The output shows 'task5 new variable'.

```
root@VM: /home/seed/Desktop
seed@pes1201800144rajdeep:~/Desktop$ printenv task5
seed@pes1201800144rajdeep:~/Desktop$ export task5='task5 new variable'
seed@pes1201800144rajdeep:~/Desktop$ printenv task5
task5 new variable
seed@pes1201800144rajdeep:~/Desktop$
```

Setting task5 as new environment variable

A terminal window titled 'Terminal' with a dark background and a vertical sidebar of application icons on the left. The terminal shows the same user 'root' at the same VM path. The user runs 'diff setuidenv env\_result'. The output indicates that the binary files differ.

```
root@VM: /home/seed/Desktop
seed@pes1201800144rajdeep:~/Desktop$ diff setuidenv env_result
Binary files setuidenv and env_result differ
seed@pes1201800144rajdeep:~/Desktop$
```

Difference between 'setuidenv' and 'env\_result'

```
root@VM: /home/seed/Desktop
seed@seed1201800144rajdeep: ~/Desktop$. /setuidenv
XDG_VTNR=7
XDG_SESSION_ID=c1
CLUTTER_IM_MODULE=xim
XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed
SESSION=ubuntu
GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1
ANDROID_HOME=/home/seed/android/android-sdk-linux
SHELL=/bin/bash
VTE_VERSION=4205
TERM=xterm-256color
DERBY_HOME=/usr/lib/jvm/java-8-oracle/db
QT_LINUX_ACCESSIBILITY_ALWAYS_ON=1
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
WINDOWID=58720266
GNOME_KEYRING_CONTROL=
UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1311
GTK_MODULES=gail:atk-bridge:unity-gtk-module
USER=seed
LD_LIBRARY_PATH=/home/seed:/home/seed/source/boost_1_64_0/stage/lib:/home/seed/source/boost_1_64_0/stage/lib:
QT_ACCESSIBILITY=1
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33:ol=40;33:cd=40;33:or=40;31: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:*.lzh=01;31:*.lzm=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7z=01;31:*.zip=01;31:*.z=01;31:*.Z=01;31:*.diz=01;31:*.gz=01;31:*.lrz=01;31:*.lrz=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:*.mpg=01;35:*.mpeg=01;35:*.m2v=01;35:*.mkv=01;35:*.webm=01;35:*.ogm=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.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:*.mid=00;36:*.midi=00;36:*.mka=00;36:*.mp3=00;36:*.mpc=00;36:*.ogg=00;36:*.ra=00;36:*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:
XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0
XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
DEFAULTS_PATH=/usr/share/pconf/ubuntu.default.path
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg
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-sdk-linux/platform-tools:/home/seed/android/ndk/android-ndk-r8d:/home/seed/.local/bin:/home/seed/android/android-sdk-linux/tools:/home/seed/android/android-sdk-linux/platform-tools:/home/seed/android/ndk/android-ndk-r8d:/home/seed/.local/bin
DESKTOP_SESSION=ubuntu
QT_QPA_PLATFORMTHEME=appmenu-qt5
QT_IM_MODULE=ibus
task5=task5 new variable
JOB=unity-settings-daemon
PWD=/home/seed/Desktop
XDG_SESSION_TYPE=x11
JAVA_HOME=/usr/lib/jvm/java-8-oracle
XMODIFIERS=@im=ibus
```

Executing the program after doing steps 2 and 3

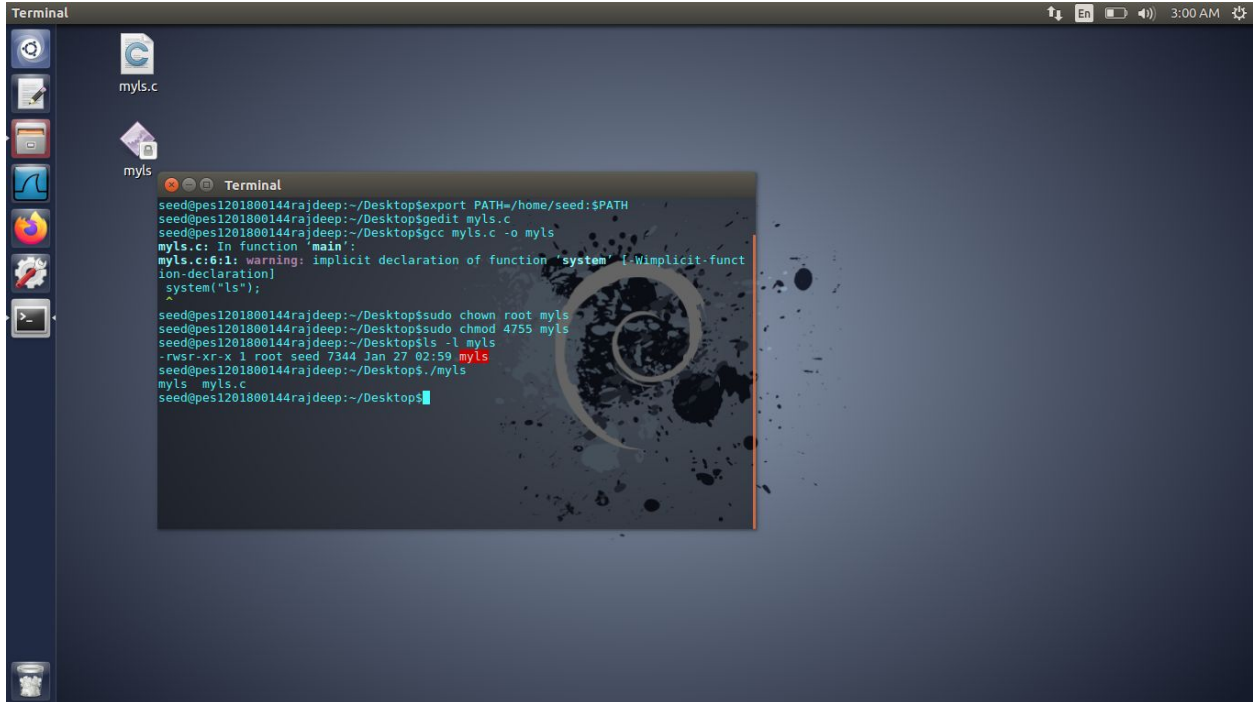
Observation Task 5:

The set-UID program does not inherit all environment variables like LD\_LIBRARY\_PATH. So we have to export LD\_LIBRARY\_PATH in Step 3 of this task. This is because RUID(real user ID) and EUID(effective user ID) are different.

=====

## TASK 6: The PATH environment variable and Set-UID programs

### Screenshots Task 6:



```
Terminal
seed@pes1201800144rajdeep:~/Desktop$ export PATH=/home/seed:$PATH
seed@pes1201800144rajdeep:~/Desktop$ gedit myls.c
seed@pes1201800144rajdeep:~/Desktop$ gcc myls.c -o myls
myls.c: In function 'main':
myls.c:6:11: warning: implicit declaration of function 'system' [-Wimplicit-function-declaration]
system("ls");
^
seed@pes1201800144rajdeep:~/Desktop$ sudo chown root myls
seed@pes1201800144rajdeep:~/Desktop$ sudo chmod 4755 myls
seed@pes1201800144rajdeep:~/Desktop$ ls -l myls
-rwsr-xr-x 1 root seed 7344 Jan 27 02:59 myls
seed@pes1201800144rajdeep:~/Desktop$ ./mysls
mysls myls.c
seed@pes1201800144rajdeep:~/Desktop$
```

Changing PATH environment variable, compiling the code and making the owner as root and changing permissions using chown and chmod

```
Terminal
root@VM: /home/seed/Desktop
seed@pes1201800144rajdeep:~/Desktop$ gcc ls.c -o ls
seed@pes1201800144rajdeep:~/Desktop$ rm /bin/sh
rm: cannot remove '/bin/sh': Permission denied
seed@pes1201800144rajdeep:~/Desktop$ sudo rm /bin/sh
seed@pes1201800144rajdeep:~/Desktop$ ln -s /bin/zsh /bin/sh
ln: failed to create symbolic link '/bin/sh': Permission denied
seed@pes1201800144rajdeep:~/Desktop$ sudo ln -s /bin/zsh /bin/sh
seed@pes1201800144rajdeep:~/Desktop$ echo $PATH
/home/seed:/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin:/usr/lib/jvm/java-8-oracle/bin:/usr/lib/jvm/java-8-oracle/db/bin:/usr/lib/jvm/java-8-oracle/jre/bin:/home/seed/android/android-sdk-linux/tools:/home/seed/android/android-sdk-linux/platform-tools:/home/seed/android-ndk/android-ndk-r8d:/home/seed/.local/bin
seed@pes1201800144rajdeep:~/Desktop$ ./ls

This is my ls Program

my real Uid is :1000
My Effective uid is:1000
seed@pes1201800144rajdeep:~/Desktop$
```

Removing /bin/sh and then using 'ln -s' for symbolic linking /bin/zsh to /bin/sh. Then exporting environment variable PATH to the current working directory and executing the program.

## Observation Task 6:

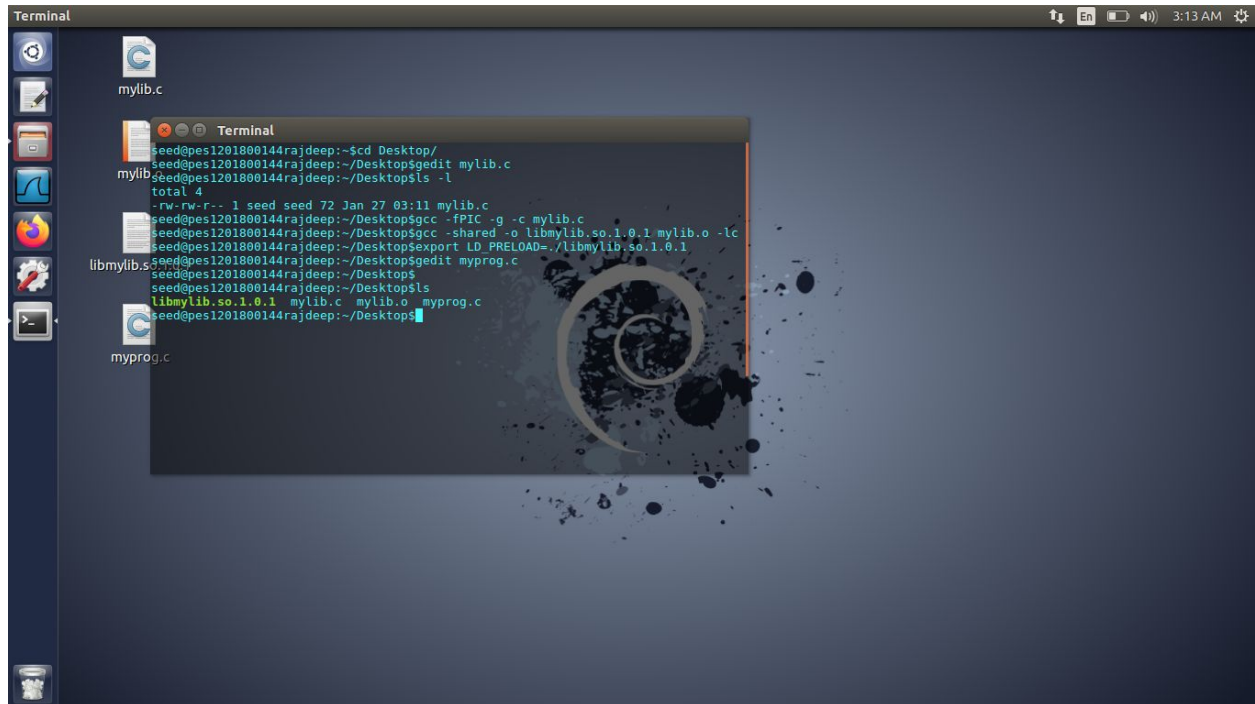
system() call with Set-UID is dangerous in terms of security as we can run our own program in place of the system's function call. For eg. in this example, our 'ls' program is executing instead of bash shell's 'ls' command.

=====



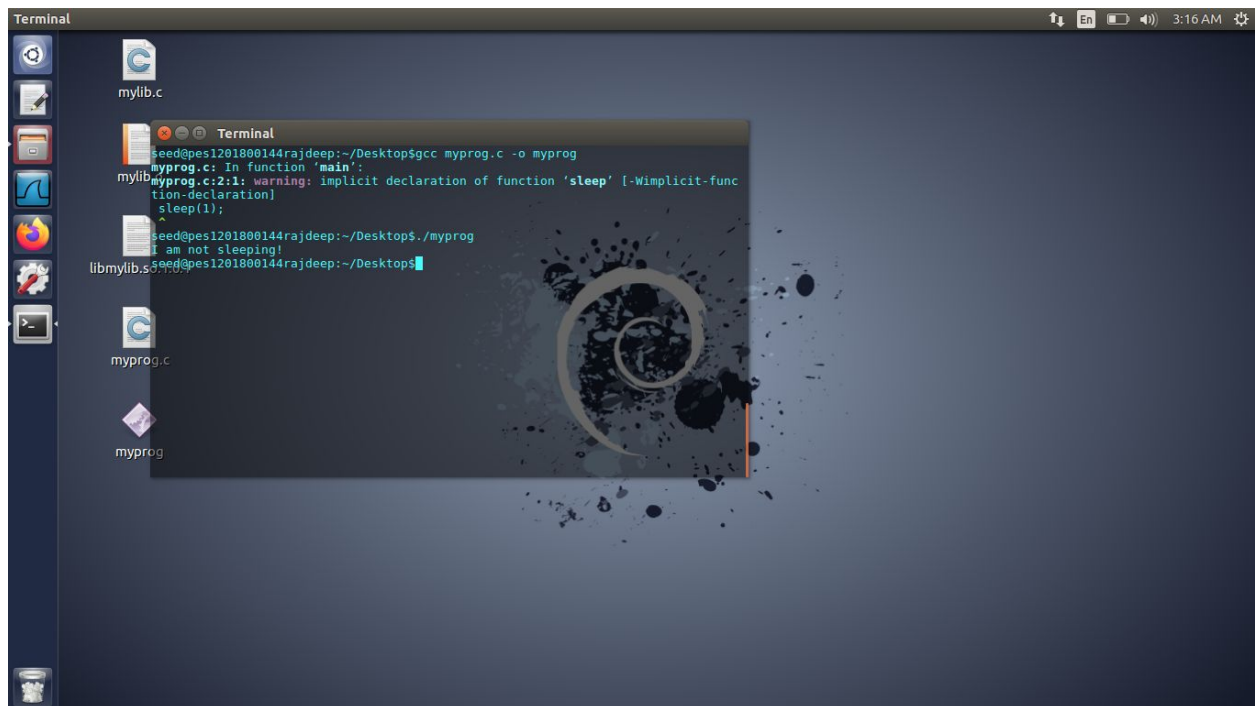
## TASK 7: The LD\_PRELOAD variable and Set-UID programs

### Screenshots Task 7:



```
Terminal
seed@pes1201800144rajdeep:~$ cd Desktop/
seed@pes1201800144rajdeep:~/Desktop$ gedit mylib.c
mylib$ seed@pes1201800144rajdeep:~/Desktop$ ls -l
total 4
-rw-rw-r-- 1 seed seed 72 Jan 27 03:11 mylib.c
seed@pes1201800144rajdeep:~/Desktop$ gcc -fPIC -g -c mylib.c
seed@pes1201800144rajdeep:~/Desktop$ gcc -shared -o libmylib.so.1.0.1 mylib.o -lc
seed@pes1201800144rajdeep:~/Desktop$ export LD_PRELOAD=./libmylib.so.1.0.1
libmylib$ seed@pes1201800144rajdeep:~/Desktop$ gedit myprog.c
seed@pes1201800144rajdeep:~/Desktop$
seed@pes1201800144rajdeep:~/Desktop$ ls
libmylib.so.1.0.1 mylib.c mylib.o myprog.c
seed@pes1201800144rajdeep:~/Desktop$
```

Setting LD\_PRELOAD to libmylib.so.1.0.1 executable file.



```
Terminal
seed@pes1201800144rajdeep:~/Desktop$ gcc myprog.c -o myprog
myprog.c: In function 'main':
myprog.c:2:1: warning: implicit declaration of function 'sleep' [-Wimplicit-function-declaration]
  sleep(1);
  ^
seed@pes1201800144rajdeep:~/Desktop$ ./myprog
I am not sleeping!
seed@pes1201800144rajdeep:~/Desktop$
```

Running the program in user mode.

The problem here is that the 'sleep' command should make the system sleep instead of executing the function with the same name.

```
root@VM: /home/seed/Desktop
root@VM:/home/seed/Desktop# whoami
root
root@VM:/home/seed/Desktop# gcc myprog.c -o myprog
myprog.c: In function 'main':
myprog.c:2:1: warning: implicit declaration of function 'sleep' [-Wimplicit-function-declaration]
sleep(1);
^
root@VM:/home/seed/Desktop# chmod 4755 myprog
root@VM:/home/seed/Desktop# ls -l myprog
-rwsr-xr-x 1 root root 7348 Jan 27 03:20 myprog
root@VM:/home/seed/Desktop# export LD_PRELOAD=./libmylib.so.1.0.1
root@VM:/home/seed/Desktop# exit
seed@pes1201800144rajdeep:~/Desktop$ ls -l myprog
-rwsr-xr-x 1 root root 7348 Jan 27 03:20 myprog
seed@pes1201800144rajdeep:~/Desktop$ export LD_PRELOAD=./libmylib.so.1.0.1
seed@pes1201800144rajdeep:~/Desktop$ whoami
seed libmylib.so.1.0.1
seed@pes1201800144rajdeep:~/Desktop$ ./myprog
seed@pes1201800144rajdeep:~/Desktop$ gcc myprog.c -o myprog
seed@pes1201800144rajdeep:~/Desktop$ rm sysexecenv.c
seed@pes1201800144rajdeep:~/Desktop$
seed@pes1201800144rajdeep:~/Desktop$ ./myprog
myprog.c: In function 'main':
myprog.c:2:1: warning: implicit declaration of function 'sleep' [-Wimplicit-function-declaration]
sleep(1);
^
seed@pes1201800144rajdeep:~/Desktop$ ./myprog
I am not sleeping!
seed@pes1201800144rajdeep:~/Desktop$ sudo su
root@VM:/home/seed/Desktop# gcc myprog.c -o myprog
myprog.c: In function 'main':
myprog.c:2:1: warning: implicit declaration of function 'sleep' [-Wimplicit-function-declaration]
sleep(1);
^
root@VM:/home/seed/Desktop# chmod 4755 myprog
root@VM:/home/seed/Desktop# ls -l myprog
-rwsr-xr-x 1 root root 7348 Jan 27 03:25 myprog
root@VM:/home/seed/Desktop# export LD_PRELOAD=./mylib.c mylib.o myprog myprog.c
root@VM:/home/seed/Desktop# export LD_PRELOAD=./libmylib.so.1.0.1
root@VM:/home/seed/Desktop# exit
seed@pes1201800144rajdeep:~/Desktop$ ls -l myprog
-rwsr-xr-x 1 root root 7348 Jan 27 03:25 myprog
seed@pes1201800144rajdeep:~/Desktop$ export LD_PRELOAD=./libmylib.so.1.0.1
seed@pes1201800144rajdeep:~/Desktop$ whoami
seed
seed@pes1201800144rajdeep:~/Desktop$ ./myprog
seed@pes1201800144rajdeep:~/Desktop$
```

Exporting LD\_PRELOAD to libmylib.so.1.0.1 in root mode and then running program in user mode which results in the desired functioning of the program (calling sleep function makes machine sleep instead of executing user defined sleep function)

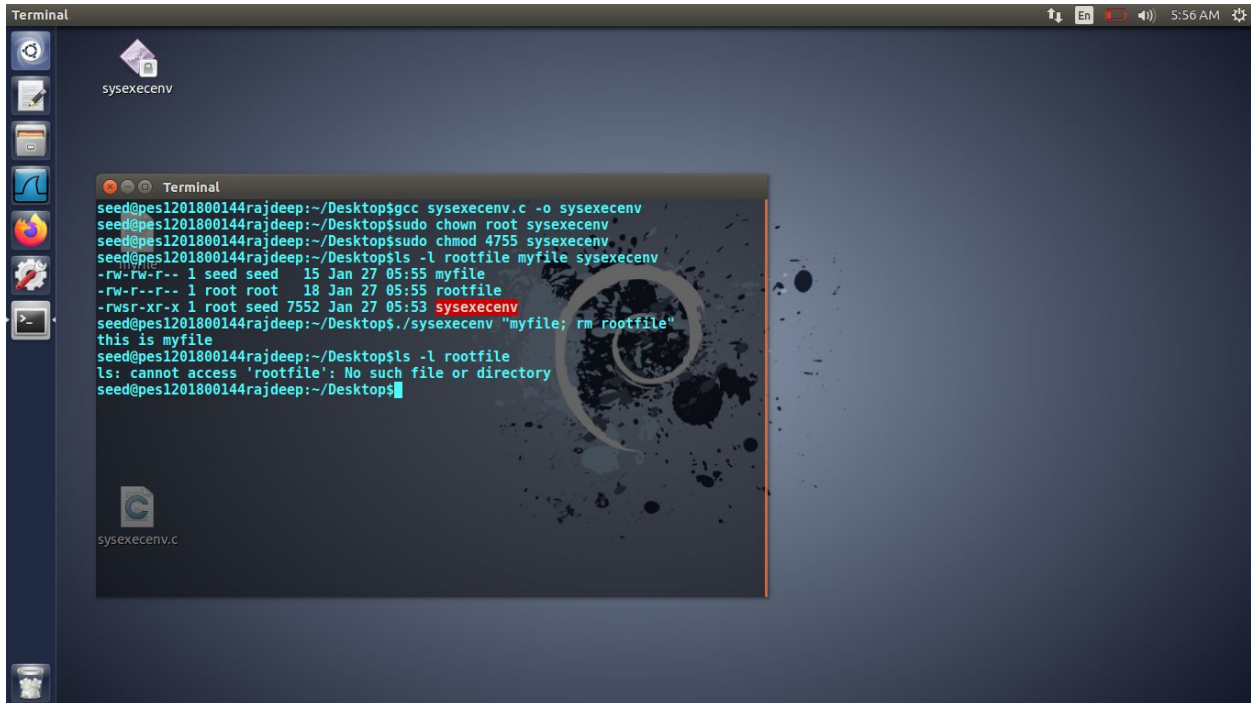
## Observation Task 7:

**LD\_PRELOAD is inherited from the program when the RUID(real user ID) is the same as the EUID(effective user ID) unlike in Task 5. When RUID and EUID are different, our program(sleep function defined is program) is executed. Further when RUID and EUID become the same after compiling in root, the system's sleep function is called which makes the system sleep.**

=====

## TASK 8: Invoking external programs using system() versus execve()

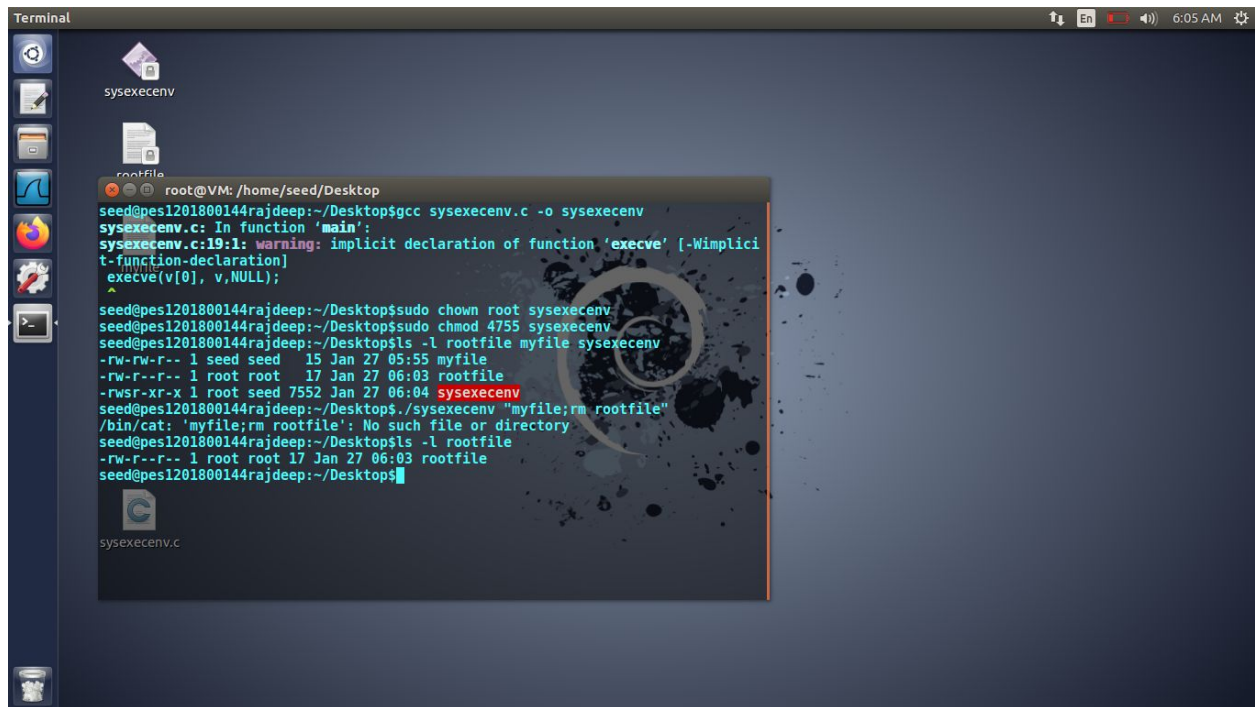
### Screenshots Task 8:



```
Terminal
sysexecenv

seed@pes1201800144rajdeep:~/Desktop$ gcc sysexecenv.c -o sysexecenv
seed@pes1201800144rajdeep:~/Desktop$ sudo chown root sysexecenv
seed@pes1201800144rajdeep:~/Desktop$ sudo chmod 4755 sysexecenv
seed@pes1201800144rajdeep:~/Desktop$ ls -l rootfile myfile sysexecenv
-rw-rw-r-- 1 seed seed 15 Jan 27 05:55 myfile
-rw-r--r-- 1 root root 18 Jan 27 05:55 rootfile
-rwsr-xr-x 1 root seed 7552 Jan 27 05:53 sysexecenv
seed@pes1201800144rajdeep:~/Desktop$ ./sysexecenv "myfile; rm rootfile"
this is myfile
seed@pes1201800144rajdeep:~/Desktop$ ls -l rootfile
ls: cannot access 'rootfile': No such file or directory
seed@pes1201800144rajdeep:~/Desktop$
```

Compiling the code and making root as owner and changing permissions using chown and chmod. Using 'rm' command in user mode removes the root permitted file. This is because of using system() call.



```
Terminal
root@VM: /home/seed/Desktop
seed@pes1201800144rajdeep:~/Desktop$ gcc sysexecenv.c -o sysexecenv
sysexecenv.c: In function 'main':
sysexecenv.c:19:1: warning: implicit declaration of function 'execve' [-Wimplicit-function-declaration]
  execve(v[0], v, NULL);
  ^
seed@pes1201800144rajdeep:~/Desktop$ sudo chown root sysexecenv
seed@pes1201800144rajdeep:~/Desktop$ sudo chmod 4755 sysexecenv
seed@pes1201800144rajdeep:~/Desktop$ ls -l rootfile myfile sysexecenv
-rw-rw-r-- 1 seed seed 15 Jan 27 05:55 myfile
-rw-r--r-- 1 root root 17 Jan 27 06:03 rootfile
-rwsr-xr-x 1 root seed 7552 Jan 27 06:04 sysexecenv
seed@pes1201800144rajdeep:~/Desktop$ ./sysexecenv "myfile;rm rootfile"
/bin/cat: 'myfile;rm rootfile': No such file or directory
seed@pes1201800144rajdeep:~/Desktop$ ls -l rootfile
-rw-r--r-- 1 root root 17 Jan 27 06:03 rootfile
seed@pes1201800144rajdeep:~/Desktop$
```

Doing the same above but this time using `execve()` instead of `system()` solves the problem and doesn't allow non-root users to delete root permitted files.

## Observation Task 8:

- `system()` allows Bob to modify the files as superuser
- `execve()` does not let Bob to modify the files as superuser

This is because `system()` function call invokes a shell which then executes the command whereas `execve()` directly executes function call.

**In this case, `system()` call invokes a new shell with root permissions(root shell) which can read, modify and delete files which makes it dangerous. Whereas in case of `execve()` call, the root shell is never invoked so permission to modify or delete is not given to Bob.**

=====

## TASK 9: Capability Leaking

```
Terminal
seed@pes1201800144rajdeep:~/Desktop$ cd Desktop/
seed@pes1201800144rajdeep:~/Desktop$ gcc capleak.c -o capleak
capleak.c:10: warning: implicit declaration of function 'sleep' [-Wimplicit-function-declaration]
sleep(2);
^
capleak.c:24:1: warning: implicit declaration of function 'setuid' [-Wimplicit-function-declaration]
setuid(getuid()); /* getuid()
^
capleak.c:24:8: warning: implicit declaration of function 'getuid' [-Wimplicit-function-declaration]
setuid(getuid()); /* getuid()
^
capleak.c:26:4: warning: implicit declaration of function 'fork' [-Wimplicit-function-declaration]
if(fork()) { /* In the parent
^
capleak.c:28:2: warning: implicit declaration of function 'close' [-Wimplicit-function-declaration]
close(fd);
^
capleak.c:36:2: warning: implicit declaration of function 'write' [-Wimplicit-function-declaration]
write(fd, "Malicious Data\n", 15);
^
seed@pes1201800144rajdeep:~/Desktop$ sudo chown root capleak
seed@pes1201800144rajdeep:~/Desktop$ sudo chmod 4755 capleak
seed@pes1201800144rajdeep:~/Desktop$ ls -l capleak
-rwsr-xr-x 1 root seed 7640 Jan 27 06:33 capleak
seed@pes1201800144rajdeep:~/Desktop$ cat /etc/zoo
important information
seed@pes1201800144rajdeep:~/Desktop$ ./capleak
seed@pes1201800144rajdeep:~/Desktop$ cat /etc/zoo
important information
Malicious Data
seed@pes1201800144rajdeep:~/Desktop$
```

When a process is permitted to execute privileged commands, the child process can execute malicious code. This capability leaking is done when the program is made owned by root and root permissions are given using `chown` and `chmod`.

### Observation Task 9:

**The child process executes the malicious code whereas the privileges were only meant for the parent process. This is a massive vulnerability which can be exploited.**

=====