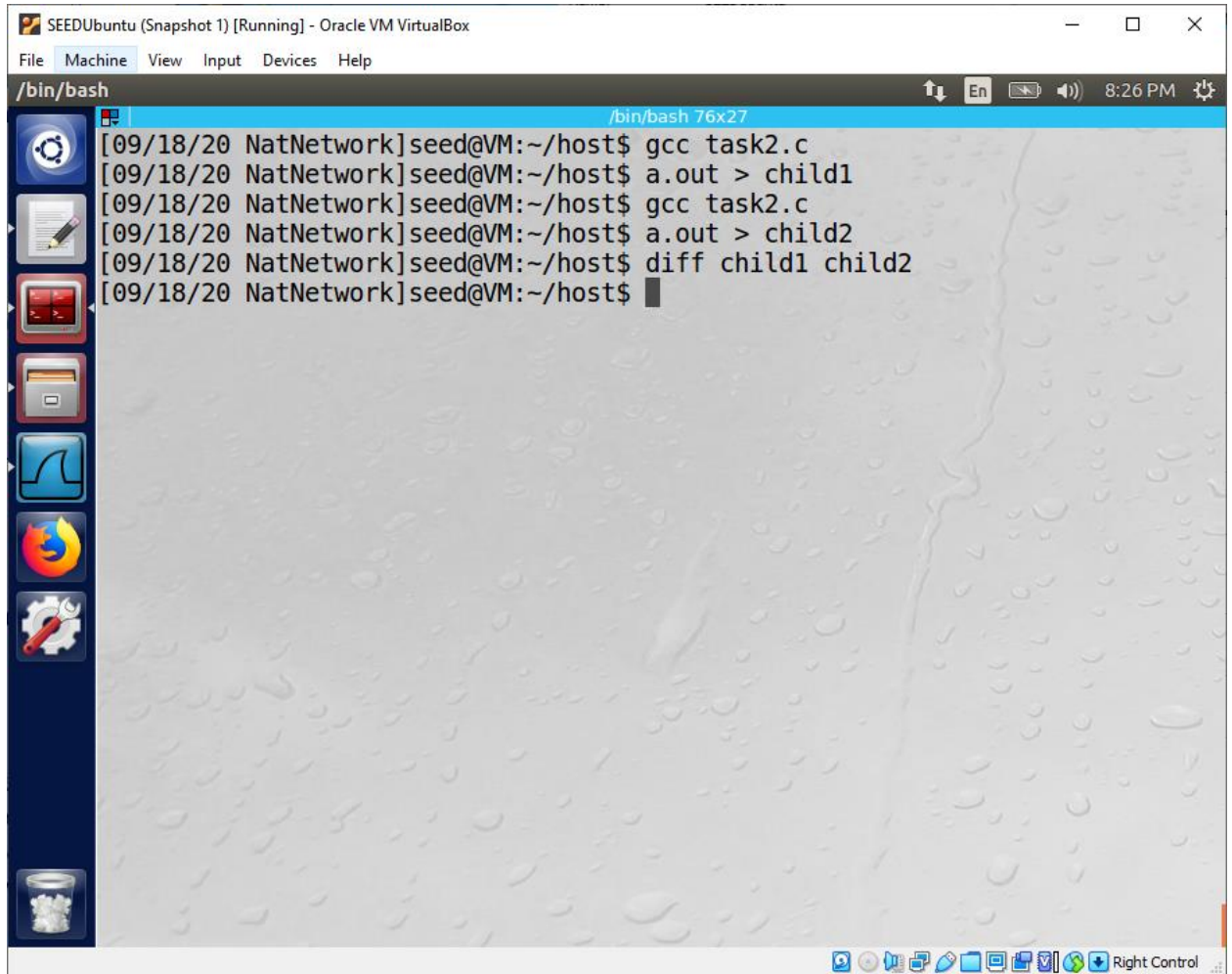


- 2.1

```
SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
/bin/bash
[09/18/20 NatNetwork]seed@VM:~$ printenv PWD
/home/seed
[09/18/20 NatNetwork]seed@VM:~$ env | grep PWD
PWD=/home/seed
[09/18/20 NatNetwork]seed@VM:~$ export foo="test"
[09/18/20 NatNetwork]seed@VM:~$ printenv foo
test
[09/18/20 NatNetwork]seed@VM:~$ unset foo
[09/18/20 NatNetwork]seed@VM:~$ printenv foo
[09/18/20 NatNetwork]seed@VM:~$
```

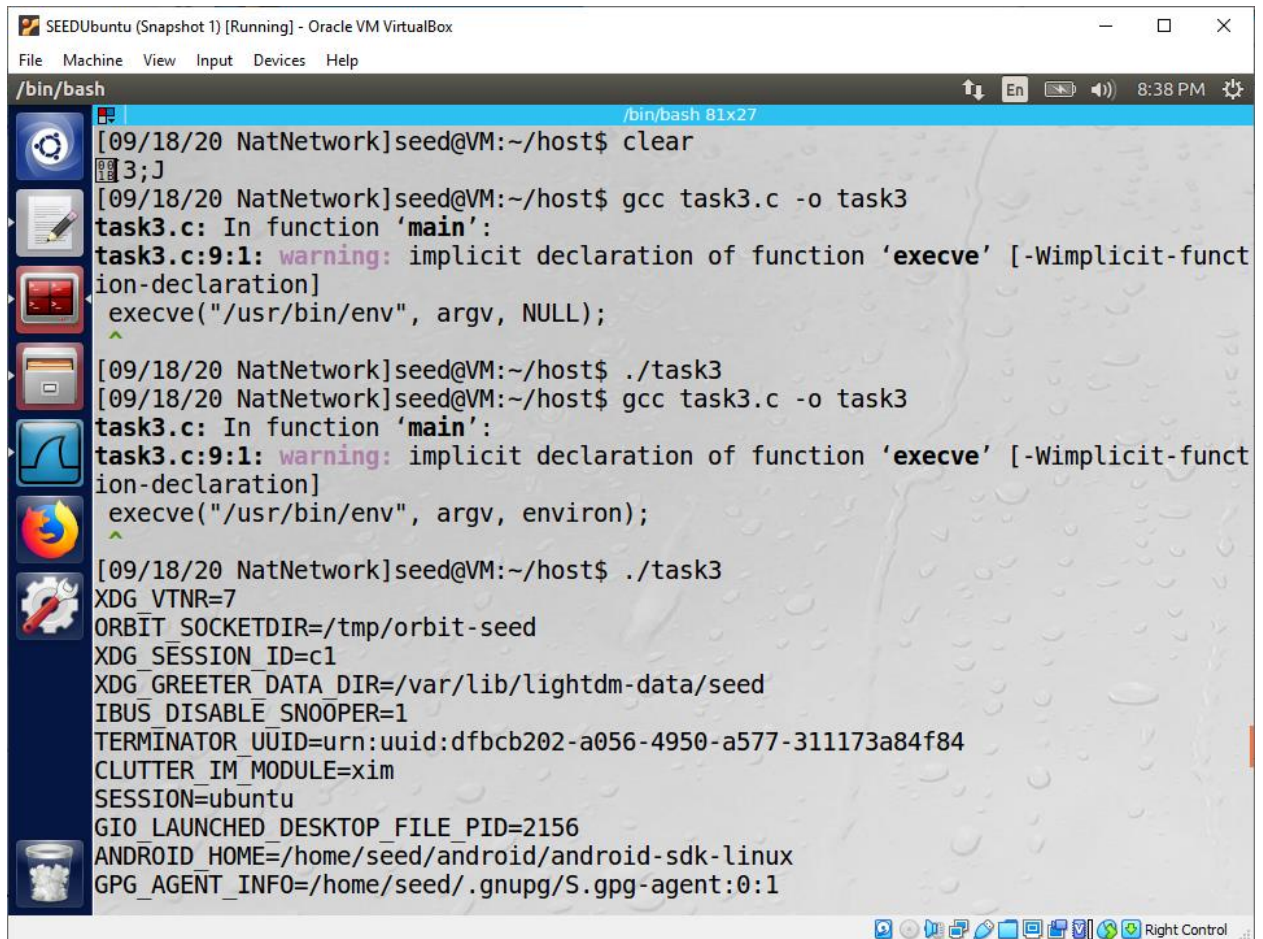
- 2.2



```
SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
/bin/bash
/bin/bash 76x27
[09/18/20 NatNetwork]seed@VM:~/host$ gcc task2.c
[09/18/20 NatNetwork]seed@VM:~/host$ a.out > child1
[09/18/20 NatNetwork]seed@VM:~/host$ gcc task2.c
[09/18/20 NatNetwork]seed@VM:~/host$ a.out > child2
[09/18/20 NatNetwork]seed@VM:~/host$ diff child1 child2
[09/18/20 NatNetwork]seed@VM:~/host$
```

- They are the same. The only difference is the process that they call the function.

- 2.3



```

SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
/bin/bash
[09/18/20 NatNetwork]seed@VM:~/host$ clear
[09/18/20 NatNetwork]seed@VM:~/host$ gcc task3.c -o task3
task3.c: In function 'main':
task3.c:9:1: warning: implicit declaration of function 'execve' [-Wimplicit-function-declaration]
  execve("/usr/bin/env", argv, NULL);
  ^
[09/18/20 NatNetwork]seed@VM:~/host$ ./task3
[09/18/20 NatNetwork]seed@VM:~/host$ gcc task3.c -o task3
task3.c: In function 'main':
task3.c:9:1: warning: implicit declaration of function 'execve' [-Wimplicit-function-declaration]
  execve("/usr/bin/env", argv, environ);
  ^
[09/18/20 NatNetwork]seed@VM:~/host$ ./task3
XDG_VTNR=7
ORBIT_SOCKETDIR=/tmp/orbit-seed
XDG_SESSION_ID=c1
XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed
IBUS_DISABLE_SNOOPER=1
TERMINATOR_UUID=urn:uuid:dfbcb202-a056-4950-a577-311173a84f84
CLUTTER_IM_MODULE=xim
SESSION=ubuntu
GIO_LAUNCHED_DESKTOP_FILE_PID=2156
ANDROID_HOME=/home/seed/android/android-sdk-linux
GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1

```

- Step 1: does not print out the environment variables
- Step 2: prints out the environment variables

- 2.4

SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

/bin/bash

/bin/bash 81x42

```
[09/18/20 NatNetwork]seed@VM:~/host$ gcc task4.c -o task4
[09/18/20 NatNetwork]seed@VM:~/host$ ./task4
LESSOPEN=| /usr/bin/lesspipe %s
GNOME_KEYRING_PID=
USER=seed
LANGUAGE=en_US
UPSTART_INSTANCE=
J2SDKDIR=/usr/lib/jvm/java-8-oracle
XDG_SEAT=seat0
SESSION=ubuntu
XDG_SESSION_TYPE=x11
COMPIZ_CONFIG_PROFILE=ubuntu-lowgfx
ORBIT_SOCKETDIR=/tmp/orbit-seed
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
GIO_LAUNCHED_DESKTOP_FILE=/usr/share/applications/terminator.desktop
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-70kAfDA4zW
GIO_LAUNCHED_DESKTOP_FILE_PID=2156
COLORTERM=gnome-terminal
GNOME_KEYRING_CONTROL=
QT_QPA_PLATFORMTHEME=appmenu-qt5
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=33554436
= ./task4
DEFAULTS_PATH=/usr/share/gconf/ubuntu.default.path
```

Right Control

- It prints out environment variable under usr/bin. Therefore, it is verified that the system() uses excel to execute /bin/sh.

From task 2.5,

At this point, I'd notice that 'chown' does not change the owner of the files for some reason, so my results might be different from what it is supposed to be. However, I followed the lab instructions, and will attach what I've done and state what I think it is supposed to be.

- 2.5

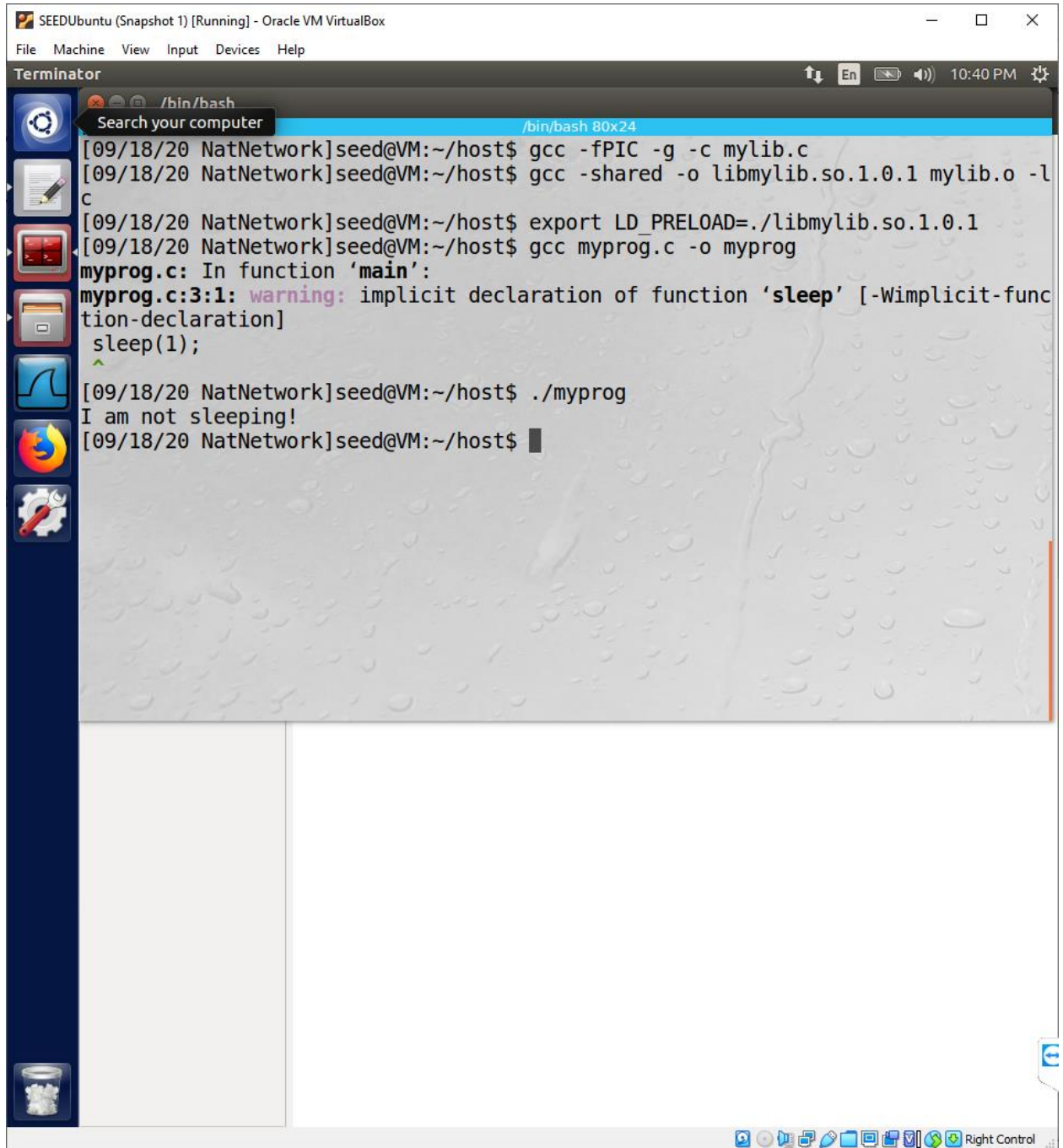
```
SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator 9:17 PM
/bin/bash
LESSOPEN=| /usr/bin/lesspipe %s
INSTANCE=
UPSTART_JOB=unity7
XDG_RUNTIME_DIR=/run/user/1000
DISPLAY=:0
XDG_CURRENT_DESKTOP=Unity
GTK_IM_MODULE=ibus
J2REDIR=/usr/lib/jvm/java-8-oracle/jre
LESSCLOSE=/usr/bin/lesspipe %s %s
XAUTHORITY=/home/seed/.Xauthority
COLORTERM=gnome-terminal
_=./a.out
OLDPWD=/home/seed
[09/18/20 NatNetwork]seed@VM:~/host$ ls -l task5s1.c
-rwxrwxrwx 1 seed seed 153 Sep 18 21:07 task5s1.c
[09/18/20 NatNetwork]seed@VM:~/host$ sudo chown root task5s1
[09/18/20 NatNetwork]seed@VM:~/host$ ls -l task5s1.c
-rwxrwxrwx 1 seed seed 153 Sep 18 21:07 task5s1.c
[09/18/20 NatNetwork]seed@VM:~/host$ chmod 4755 task5s1
[09/18/20 NatNetwork]seed@VM:~/host$ ls -l task5s1.c
-rwxrwxrwx 1 seed seed 153 Sep 18 21:07 task5s1.c
[09/18/20 NatNetwork]seed@VM:~/host$
[09/18/20 NatNetwork]seed@VM:~/host$
[09/18/20 NatNetwork]seed@VM:~/host$ export PATH
[09/18/20 NatNetwork]seed@VM:~/host$ LD_LIBRARY_PATH=/usr/share/
[09/18/20 NatNetwork]seed@VM:~/host$ export LIBRARY_PATH
[09/18/20 NatNetwork]seed@VM:~/host$
[09/18/20 NatNetwork]seed@VM:~/host$ MYNAME=task5name
[09/18/20 NatNetwork]seed@VM:~/host$
[09/18/20 NatNetwork]seed@VM:~/host$ export MYNAME
[09/18/20 NatNetwork]seed@VM:~/host$
[09/18/20 NatNetwork]seed@VM:~/host$ ./a.out
XDG_VTNR=7
```

C Tab Width: 8 Ln 11, Col 2 INS


```
SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
/bin/bash 80x34
:*.midi=00;36:*.mka=00;36:*.mp3=00;36:*.mpc=00;36:*.ogg=00;36:*.ra=00;36:*.wav=0
0;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:
QT_ACCESSIBILITY=1
LD_LIBRARY_PATH=/usr/share/
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.default.path
GIO_LAUNCHED_DESKTOP_FILE=/usr/share/applications/terminator.desktop
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:/hom
e/seed/android/android-ndk/android-ndk-r8d:/home/seed/.local/bin
QT_IM_MODULE=ibus
QT_QPA_PLATFORMTHEME=appmenu-qt5
XDG_SESSION_TYPE=x11
PWD=/home/seed/host
JOB=unity-settings-daemon
XMODIFIERS=@im=ibus
JAVA_HOME=/usr/lib/jvm/java-8-oracle
GNOME_KEYRING_PID=
LANG=en_US.UTF-8
GDM_LANG=en_US
MANDATORY_PATH=/usr/share/gconf/ubuntu.mandatory.path
COMPIZ_CONFIG_PROFILE=ubuntu-lowgfx
IM_CONFIG_PHASE=1
GDMSESSION=ubuntu
MYNAME=task5name
SESSIONTYPE=gnome-session
GTK2_MODULES=overlay-scrollbar
SHLVL=1
```

-
- What I expect: I am accessing the file as a non-root user. At that point, a new process was forked with root permission and the file was executed under the permission in the process. The command 'export' sets the environmental variable for all the processes in the system, which the root user also would be accessing. Then, this is how it is getting the values what we have set in the command.

- 2.6



The screenshot shows a VirtualBox window titled "SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox". Inside the window is a Linux desktop environment with a dark blue sidebar containing icons for settings, a search bar, and various applications. The main area is a terminal window titled "Terminator" with a light blue header bar showing "/bin/bash" and "80x24". The terminal output is as follows:

```
[09/18/20 NatNetwork]seed@VM:~/host$ gcc -fPIC -g -c mylib.c
[09/18/20 NatNetwork]seed@VM:~/host$ gcc -shared -o libmylib.so.1.0.1 mylib.o -lc
[09/18/20 NatNetwork]seed@VM:~/host$ export LD_PRELOAD=./libmylib.so.1.0.1
[09/18/20 NatNetwork]seed@VM:~/host$ 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);
  ^
[09/18/20 NatNetwork]seed@VM:~/host$ ./myprog
I am not sleeping!
[09/18/20 NatNetwork]seed@VM:~/host$
```

The terminal window has a search bar at the top that says "Search your computer". The desktop background is a light gray with a subtle pattern of water droplets. The bottom of the window shows a taskbar with various icons and a "Right Control" button.

- Case 1: uses LD_PRELOAD environment variable to override the sleep function.


```
SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
root@VM: /home/seed/host
root@VM: /home/seed/host 80x24
[09/18/20 NatNetwork]seed@VM:~/host$ export LD_PRELOAD=./libmylib.so.1.0.1
[09/18/20 NatNetwork]seed@VM:~/host$ gcc myprog.c -o myprog
myprog.c: In function 'main':
myprog.c:3:1: warning: implicit declaration of function 'sleep' [-Wimplicit-func
tion-declaration]
sleep(1);
^
[09/18/20 NatNetwork]seed@VM:~/host$ ./myprog
I am not sleeping!
[09/18/20 NatNetwork]seed@VM:~/host$ sudo su
root@VM:/home/seed/host# export L_PRELOAD=./libmylib.so.1.0.1
root@VM:/home/seed/host# gcc myprog.c -o myprog
myprog.c: In function 'main':
myprog.c:3:1: warning: implicit declaration of function 'sleep' [-Wimplicit-func
tion-declaration]
sleep(1);
^
root@VM:/home/seed/host# chmod u+s myprog
root@VM:/home/seed/host# ./myprog
I am not sleeping!
root@VM:/home/seed/host# exit
exit
[09/18/20 NatNetwork]seed@VM:~/host$ ./myprog
I am not sleeping!
[09/18/20 NatNetwork]seed@VM:~/host$
```

-
- Case 2(before exit): ignores the environment, so it is not overloaded. It just uses the system's own sleep function
- Case 3(after exit): uses the environment variable, and uses the overloaded sleep function

```
SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator 10:44 PM
user2@VM: /home/seed/host
user2@VM: /home/seed/host 80x24
sleep(1);
root@VM:/home/seed/host# chmod u+s myprog
root@VM:/home/seed/host# ./myprog
root@VM:/home/seed/host# exit
exit
[09/18/20 NatNetwork]seed@VM:~/host$ ./myprog
I am not sleeping!
[09/18/20 NatNetwork]seed@VM:~/host$ sudo su
root@VM:/home/seed/host# useradd -d /usr/user2 -m user2
root@VM:/home/seed/host# su user2
user2@VM:/home/seed/host$ export LD_PRELOAD=./libmylib.so.1.0.1
user2@VM:/home/seed/host$ 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);
user2@VM:/home/seed/host$ ./myprog
I am not sleeping!
user2@VM:/home/seed/host$ su seed
Password:
[09/18/20 NatNetwork]seed@VM:~/host$ ./myprog
[09/18/20 NatNetwork]seed@VM:~/host$
```

-
- Case 4: the sleep function is not overloaded.
- Conclusion: Only the program created by the user itself runs the LD_PRELOAD environment variable, overloading the sleep function.

- 2.7 (At this point, I noticed the ownership has not been changed. I tried to fix it rather to continue working on it since I could not change the ownership of any files.

```

SEEDUbuntu (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
user2@VM: /home/seed/host
user2@VM: /home/seed/host 80x24
-rwxrwxrwx 1 seed seed 4413 Sep 18 20:26 child1
-rwxrwxrwx 1 seed seed 4413 Sep 18 20:27 child2
-rwxrwxrwx 1 seed seed 7920 Sep 18 22:40 libmylib.so.1.0.1
-rwxrwxrwx 1 seed seed 159 Sep 18 22:39 mylib.c
-rwxrwxrwx 1 seed seed 2580 Sep 18 22:40 mylib.o
-rwxrwxrwx 1 seed seed 7348 Sep 18 22:44 myprog
-rwxrwxrwx 1 seed seed 50 Sep 18 22:39 myprog.c
-rwxrwxrwx 1 seed seed 0 Sep 18 23:10 sample.txt
-rwxrwxrwx 1 seed seed 7424 Sep 18 22:55 setuid
-rwxrwxrwx 1 seed seed 188 Sep 18 22:55 setuid.c
-rwxrwxrwx 1 seed seed 341 Sep 18 20:26 task2.c
-rwxrwxrwx 1 seed seed 7448 Sep 18 20:39 task3
-rwxrwxrwx 1 seed seed 184 Sep 18 20:38 task3.c
-rwxrwxrwx 1 seed seed 7348 Sep 18 20:48 task4
-rwxrwxrwx 1 seed seed 89 Sep 18 20:46 task4.c
-rwxrwxrwx 1 seed seed 7400 Sep 18 21:07 task5s1
-rwxrwxrwx 1 seed seed 153 Sep 18 21:07 task5s1.c
-rwxrwxrwx 1 seed seed 7544 Sep 18 20:20 task8
-rwxrwxrwx 1 seed seed 415 Sep 18 23:02 task8.c
drwxrwxrwx 1 seed seed 0 Sep 18 19:36 Trash-1000
root@VM:/home/seed/host# su user2
user2@VM:/home/seed/host$ ./task8
Please type a file name.
user2@VM:/home/seed/host$

```

- 2.8
- 2.9