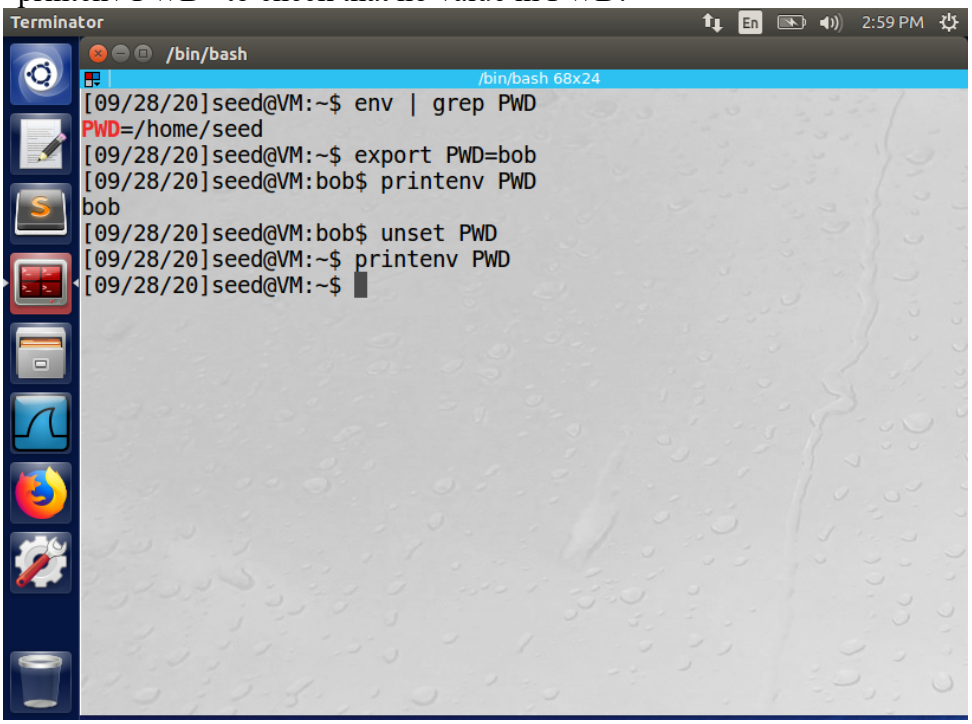
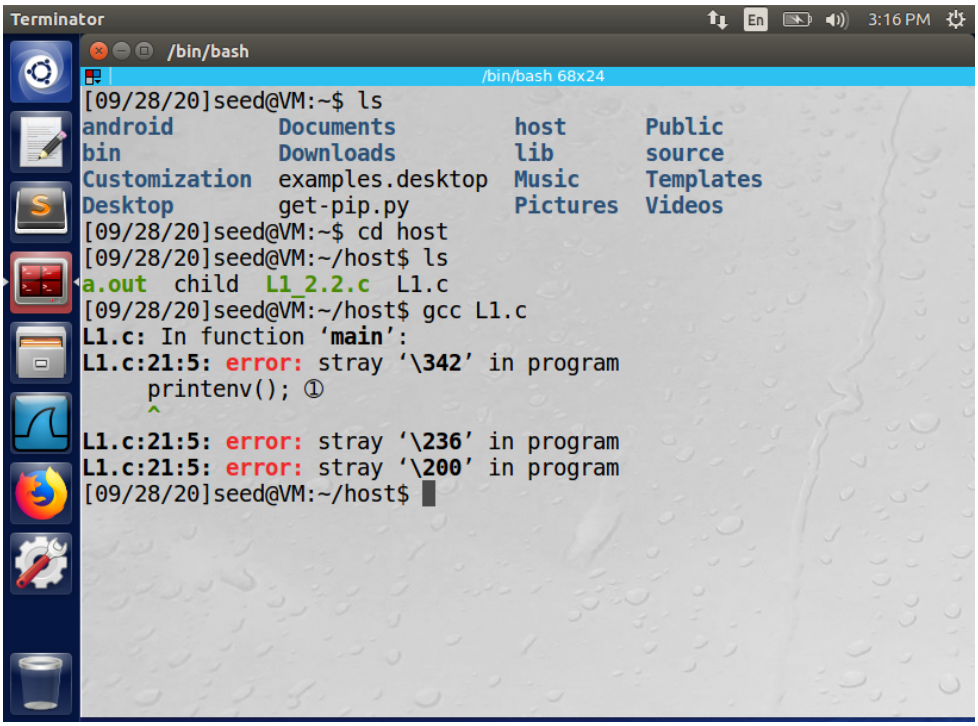
Man Tik Li
CS 377 - 001
September 28, 2020

Lab 1

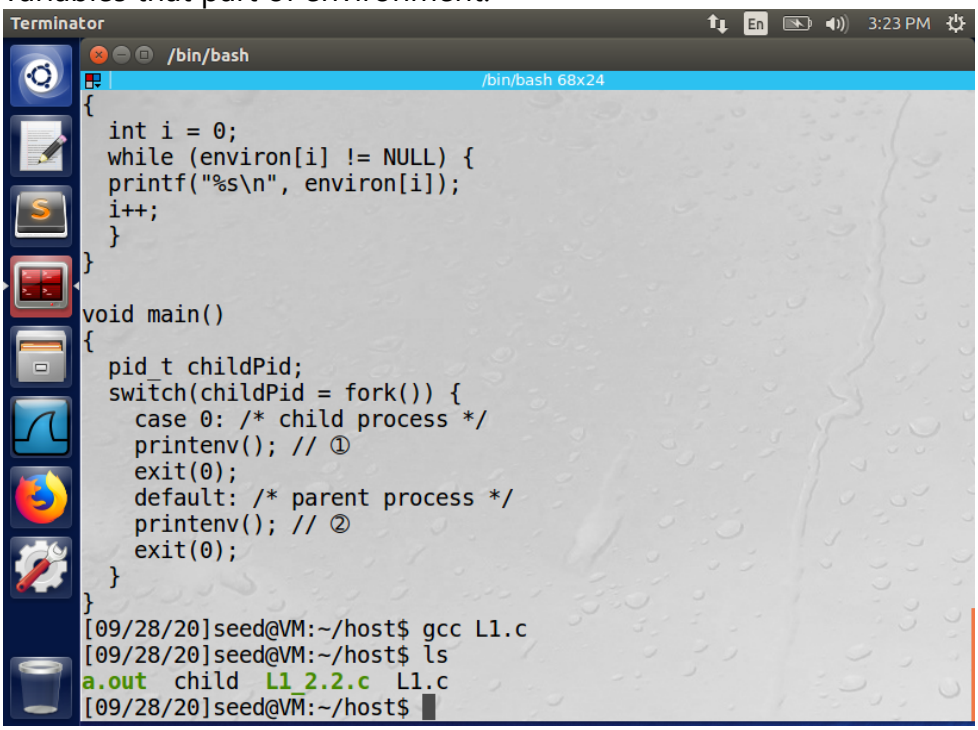
1. First use “env | grep PWD” to find the value of PWD. Then use “export” to change the value of PWD to bob and use “printenv PWD” to print out the value of PWD has changed to bob. After that, I used “unset” function to delete the variable and used “printenv PWD” to check that no value in PWD.



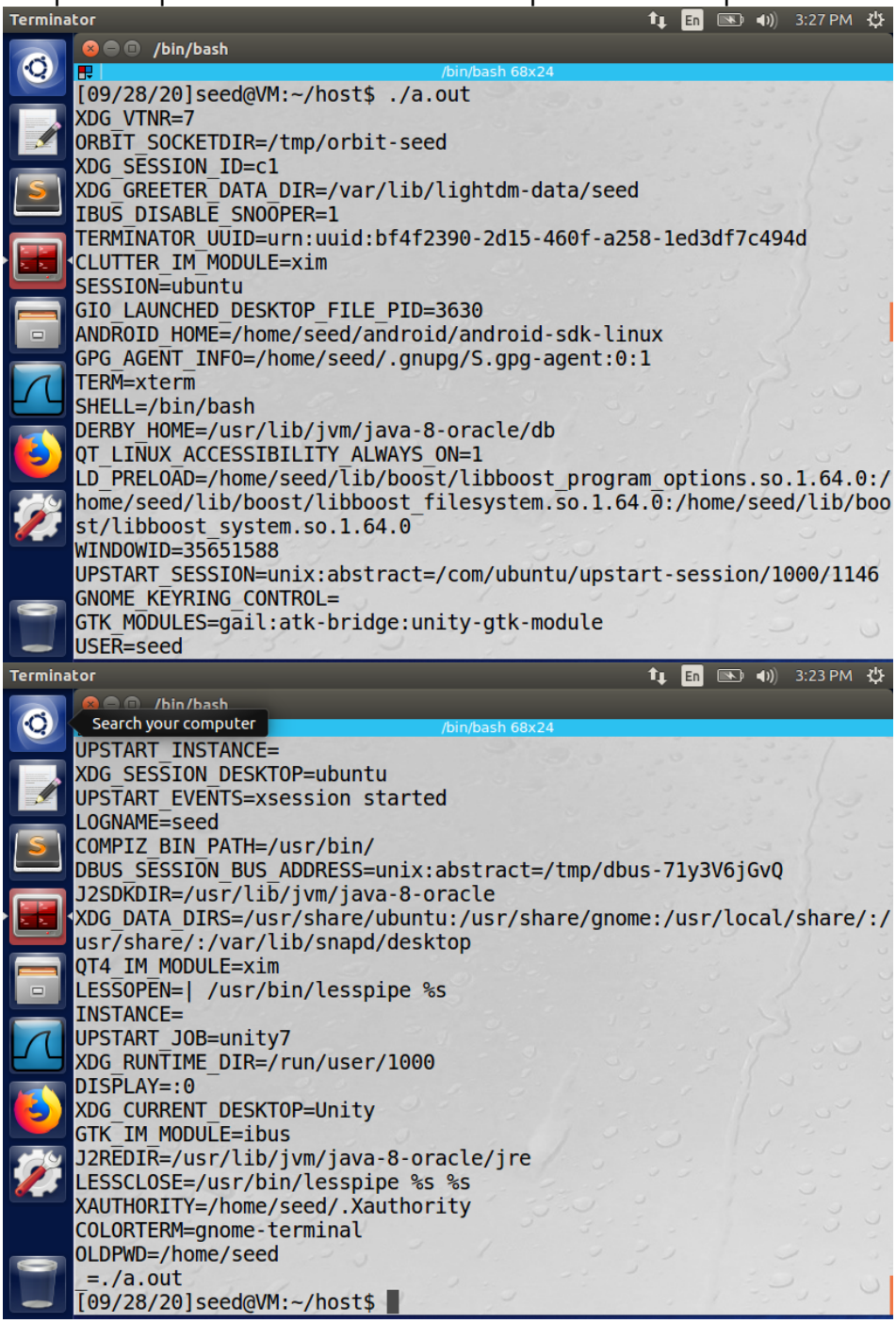
2. Step1 1: When completing the program, I got an error on printenv() because of the Line ① sign that after the printenv statement.



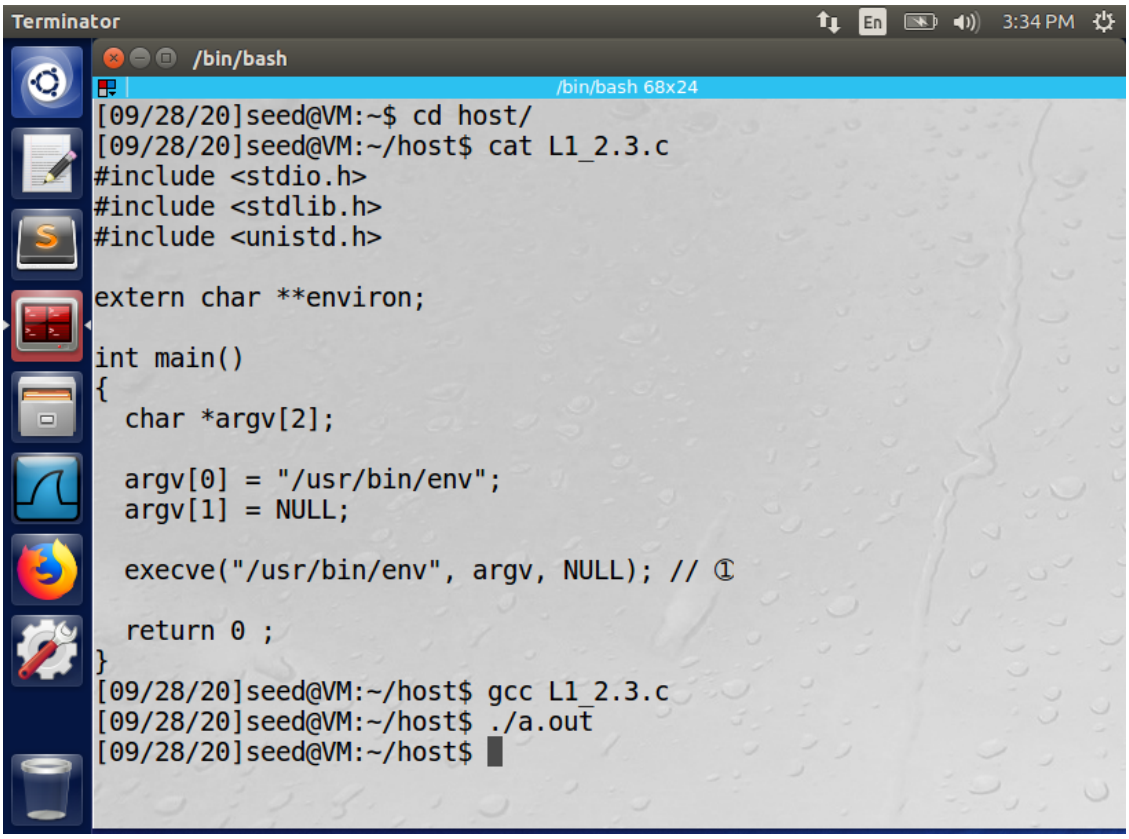
Step 2: After commenting out the Line ① and Line ②, the program successfully compiles and run. The code prints the values of the specified environment variables that part of environment.



Output: I captured the first and the last part of the output.



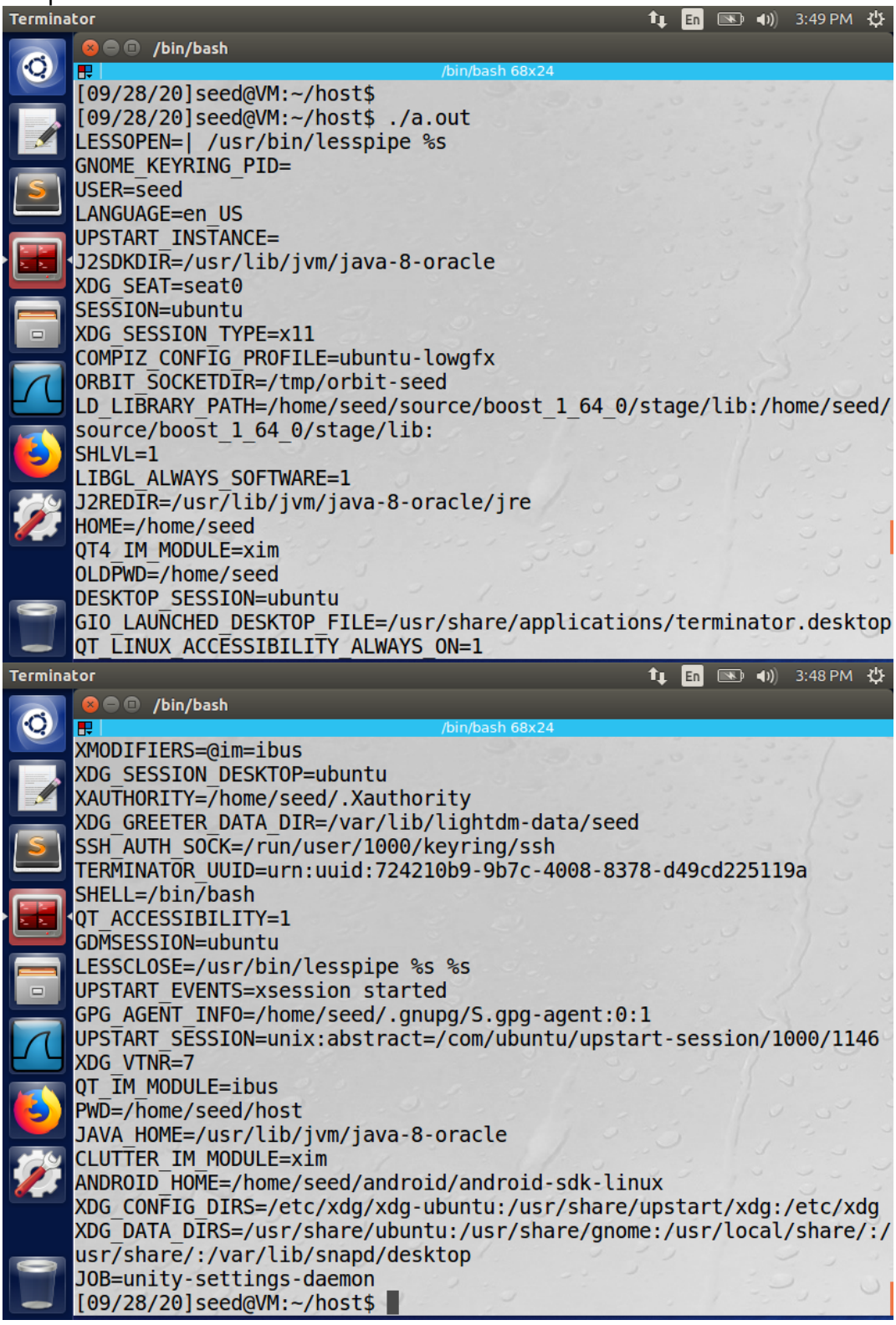
3. After compile and run the code, the program didn't print out any value from environment variables.



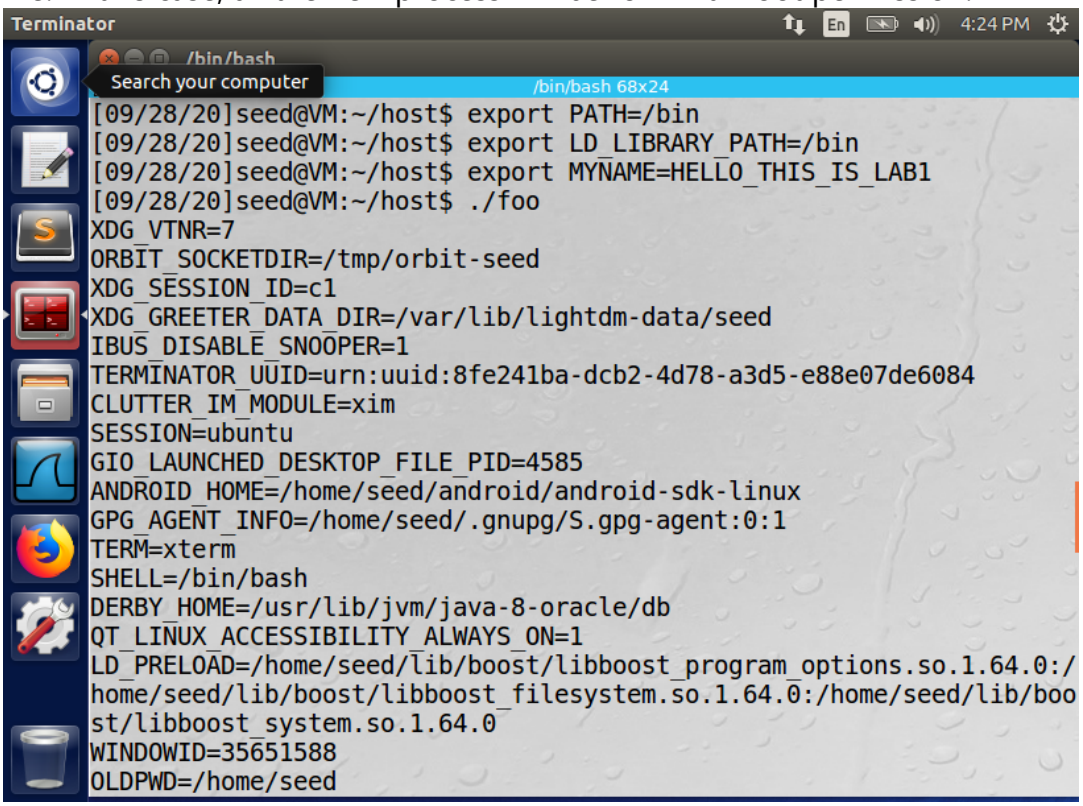
After change the third arguments in execve from NULL to environ, the program prints all the environment variables.

Conclusion: The execve() has three parameters: filename, array contains the arguments, and the envp array contains the environment variables. If set the third arguemnts in execve() to NULL, the process does not pass any environment variable. If change it to environ, it passing all the environment variables.

4. Output:

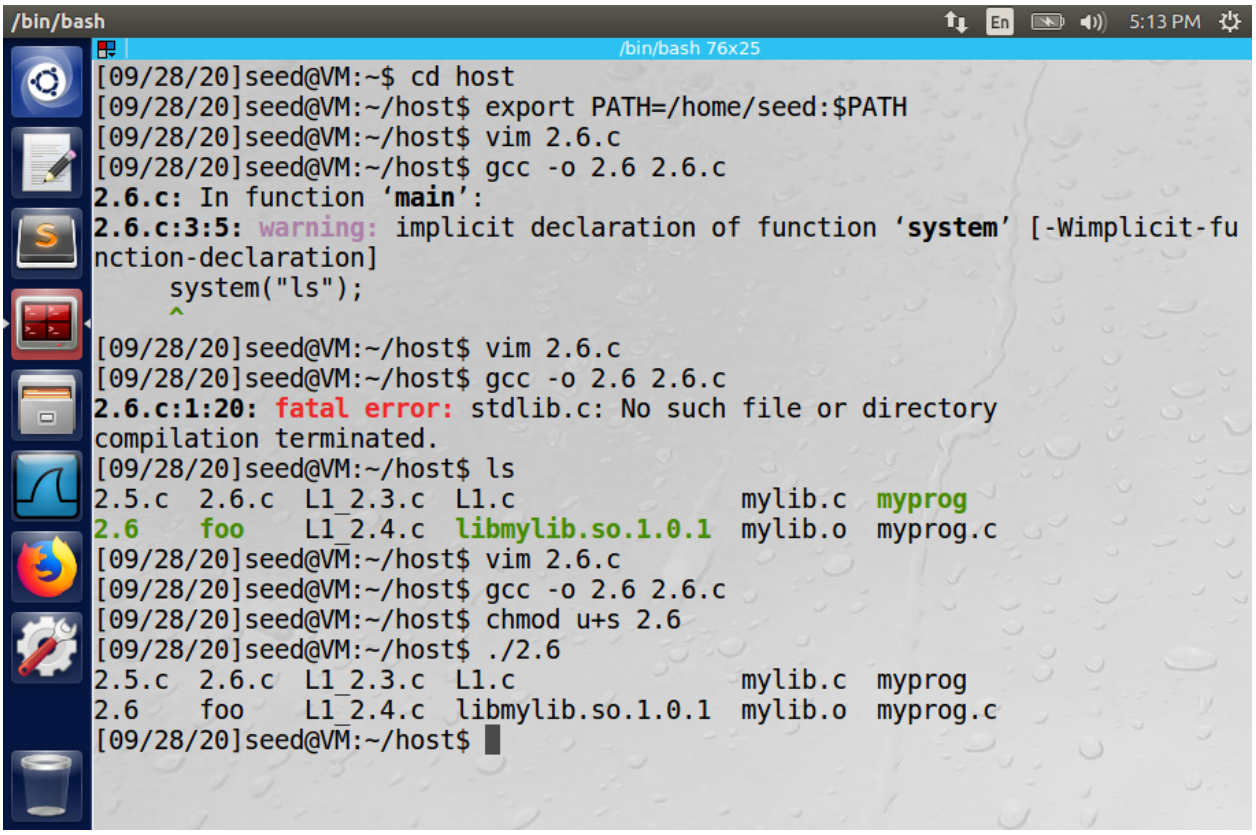

Terminator
En
3:49 PM
/bin/bash
/bin/bash 68x24
[09/28/20]seed@VM:~/host$
[09/28/20]seed@VM:~/host$ ./a.out
LESSOPEN=| /usr/bin/lesspipe %s
GNOME_KEYRING_PID=
USER=seed
LANGUAGE=en_US
UPSTART_INSTANCE=
J2SDKDIR=/usr/lib/jvm/java-8-oracle
XDG_SEAT=seat0
SESSION=ubuntu
XDG_SESSION_TYPE=x11
COMPIZ_CONFIG_PROFILE=ubuntu-lowgfx
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
Terminator
En
3:48 PM
/bin/bash
/bin/bash 68x24
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
TERMINATOR_UUID=urn:uuid:724210b9-9b7c-4008-8378-d49cd225119a
SHELL=/bin/bash
QT_ACCESSIBILITY=1
GDMSESSION=ubuntu
LESSCLOSE=/usr/bin/lesspipe %s %s
UPSTART_EVENTS=xsession started
GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1
UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1146
XDG_VTNR=7
QT_IM_MODULE=ibus
PWD=/home/seed/host
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
JOB=unity-settings-daemon
[09/28/20]seed@VM:~/host$

5. The program will change the value for PATH, LD_LIBRARY_PATH, and the user defined variable to what I defined in screenshot. The reason we can change the value and create new variable because of the ownership permission of the file has change to root. When the file is under root, any non-root user cannot access the file. In this case, all the new process will be fork with root permission.

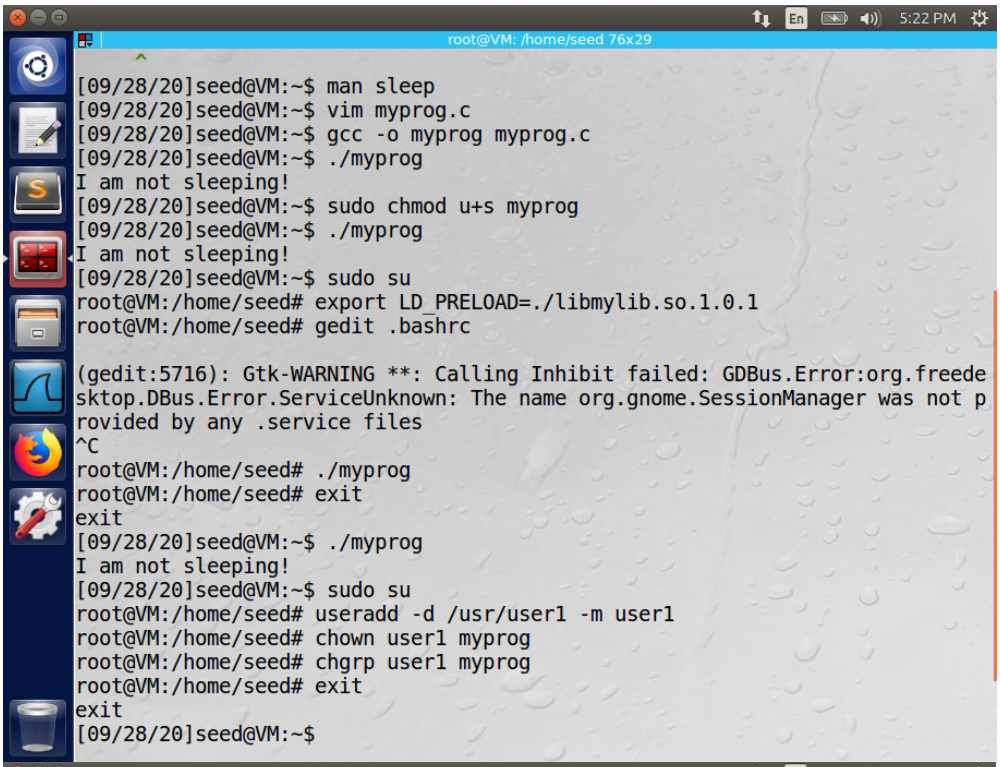


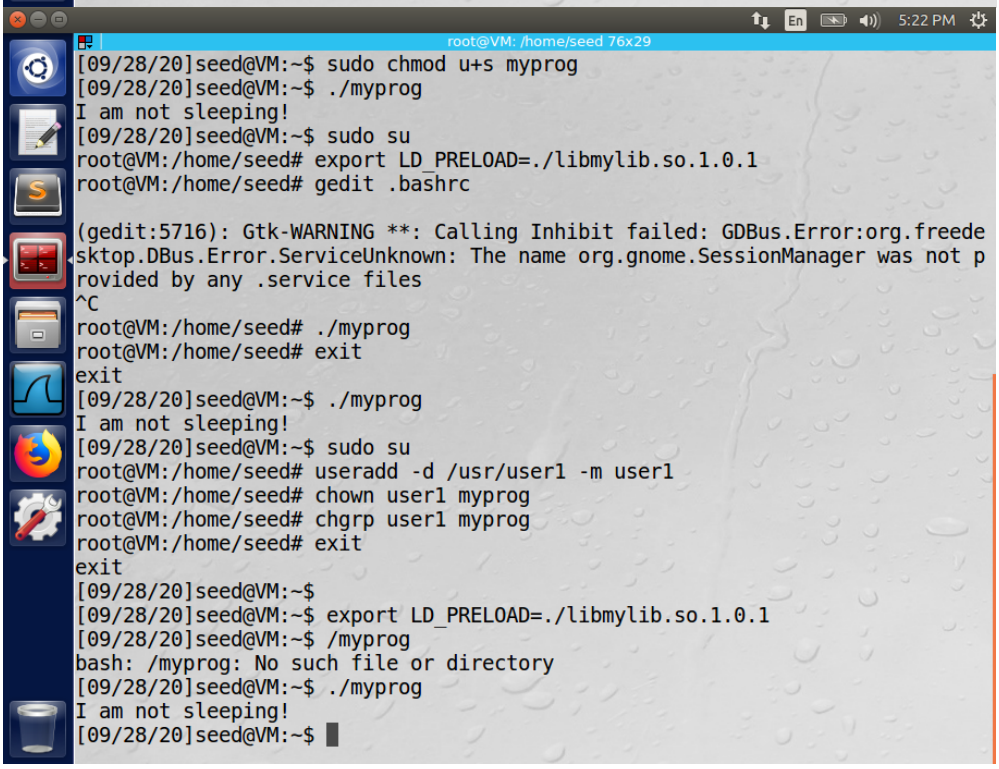

Terminator
En
4:24 PM
/bin/bash
/bin/bash 68x24
Text Editor
0;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:
PATH=/bin
XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0
XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
DEFAULTS_PATH=/usr/share/gconf/ubuntu.default.path
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=/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
Terminator
En
4:25 PM
/bin/bash
/bin/bash 68x24
Text Editor
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=/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=HELLO_THIS_IS_LAB1
SESSIONTYPE=gnome-session

6. Yes, you can let set-uid program that is owned by root to run the code. However, it is unsafe.

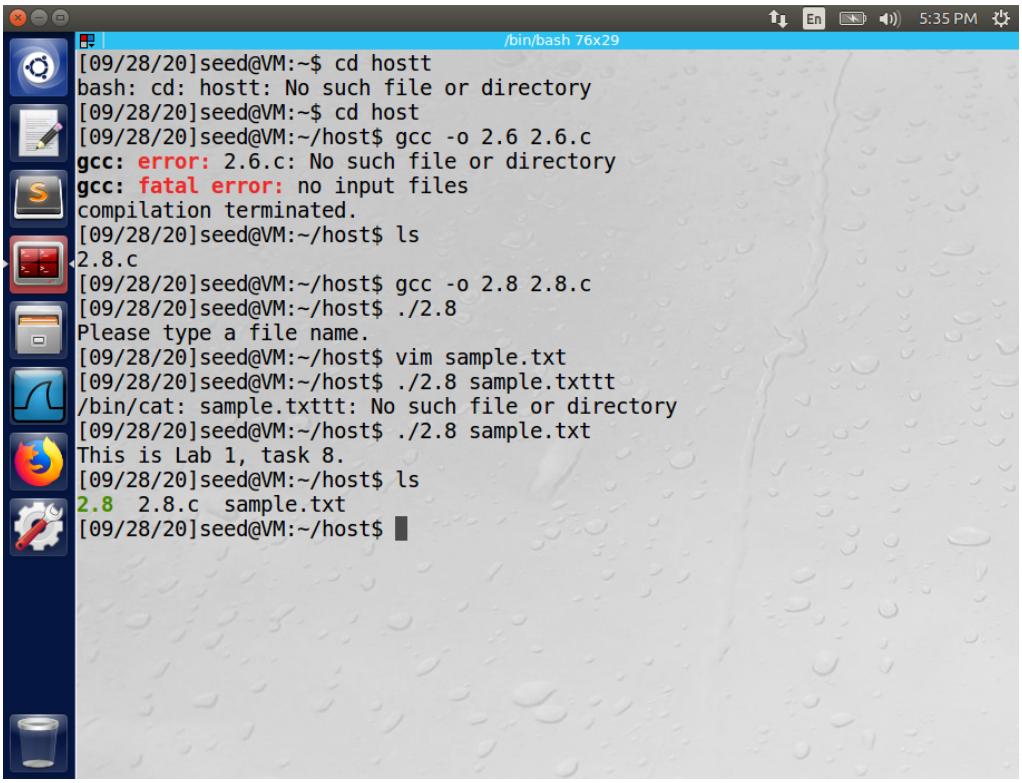


7.

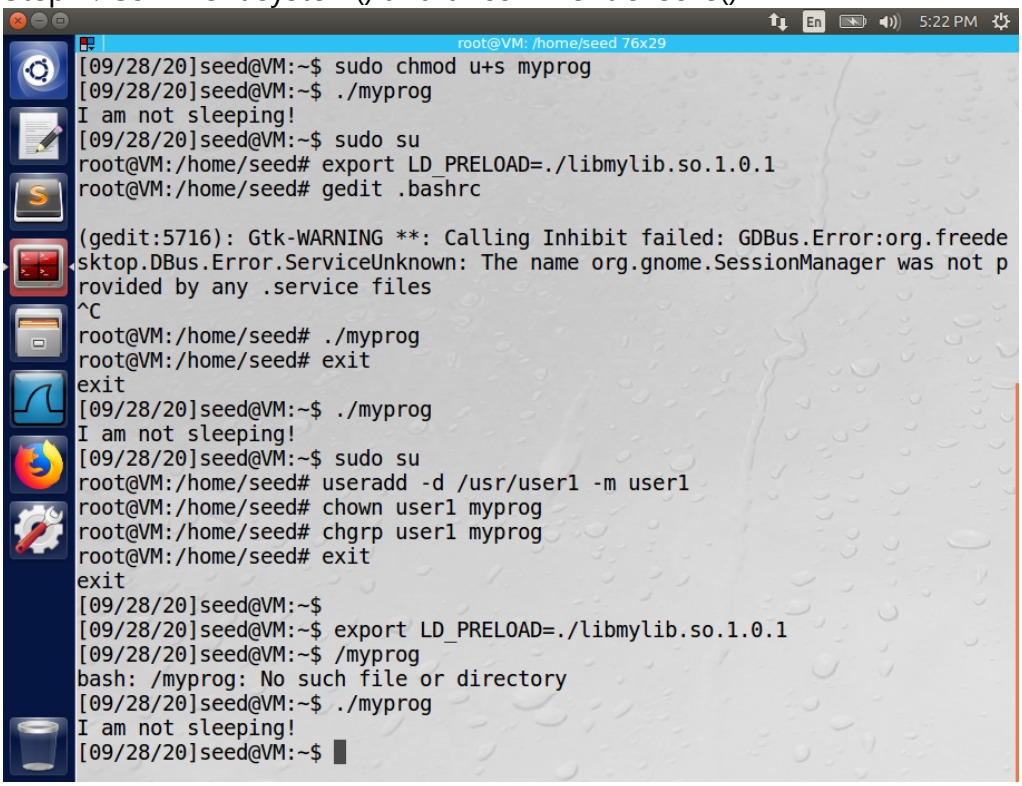

5:22 PM
root@VM: /home/seed 76x29
[09/28/20]seed@VM:~$ man sleep
[09/28/20]seed@VM:~$ vim myprog.c
[09/28/20]seed@VM:~$ gcc -o myprog myprog.c
[09/28/20]seed@VM:~$ ./myprog
I am not sleeping!
[09/28/20]seed@VM:~$ sudo chmod u+s myprog
[09/28/20]seed@VM:~$ ./myprog
I am not sleeping!
[09/28/20]seed@VM:~$ sudo su
root@VM:/home/seed# export LD_PRELOAD=./libmylib.so.1.0.1
root@VM:/home/seed# gedit .bashrc
(gedit:5716): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freede
sktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not p
rovided by any .service files
^C
root@VM:/home/seed# ./myprog
root@VM:/home/seed# exit
exit
[09/28/20]seed@VM:~$ ./myprog
I am not sleeping!
[09/28/20]seed@VM:~$ sudo su
root@VM:/home/seed# useradd -d /usr/user1 -m user1
root@VM:/home/seed# chown user1 myprog
root@VM:/home/seed# chgrp user1 myprog
root@VM:/home/seed# exit
exit
[09/28/20]seed@VM:~$


5:22 PM
root@VM: /home/seed 76x29
[09/28/20]seed@VM:~$ sudo chmod u+s myprog
[09/28/20]seed@VM:~$ ./myprog
I am not sleeping!
[09/28/20]seed@VM:~$ sudo su
root@VM:/home/seed# export LD_PRELOAD=./libmylib.so.1.0.1
root@VM:/home/seed# gedit .bashrc
(gedit:5716): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freede
sktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not p
rovided by any .service files
^C
root@VM:/home/seed# ./myprog
root@VM:/home/seed# exit
exit
[09/28/20]seed@VM:~$ ./myprog
I am not sleeping!
[09/28/20]seed@VM:~$ sudo su
root@VM:/home/seed# useradd -d /usr/user1 -m user1
root@VM:/home/seed# chown user1 myprog
root@VM:/home/seed# chgrp user1 myprog
root@VM:/home/seed# exit
exit
[09/28/20]seed@VM:~$
[09/28/20]seed@VM:~$ export LD_PRELOAD=./libmylib.so.1.0.1
[09/28/20]seed@VM:~$ /myprog
bash: /myprog: No such file or directory
[09/28/20]seed@VM:~$ ./myprog
I am not sleeping!
[09/28/20]seed@VM:~$

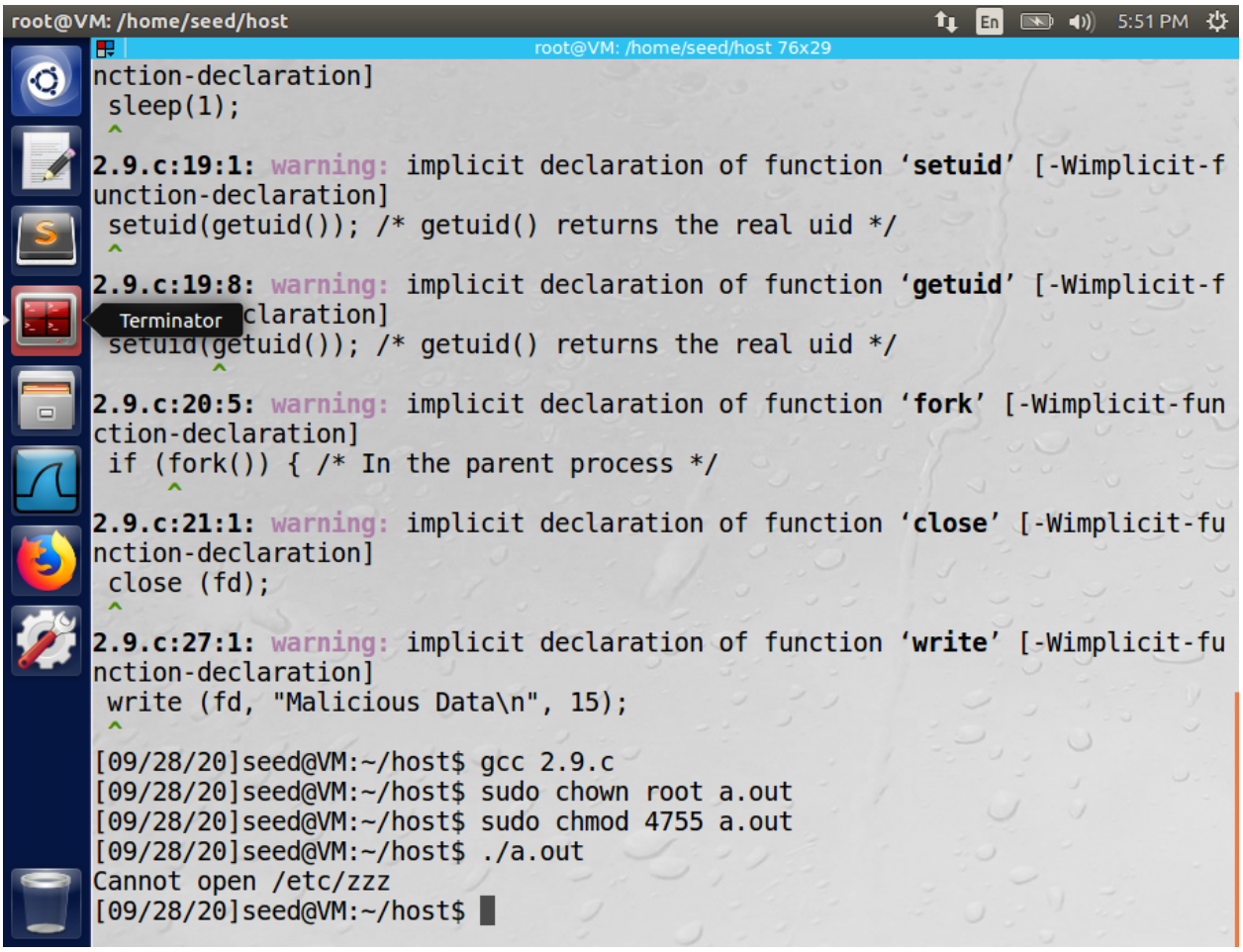
8. Step1:



Step 2: Comment system() and uncomment execve()



Yes, attacks in Step 1 still work, I can read the file content.

9. 
root@VM: /home/seed/host
En
5:51 PM
root@VM: /home/seed/host 76x29
Terminator
nction-declaration]
sleep(1);
^
2.9.c:19:1: warning: implicit declaration of function ‘setuid’ [-Wimplicit-f
unction-declaration]
setuid(getuid()); /* getuid() returns the real uid */
^
2.9.c:19:8: warning: implicit declaration of function ‘getuid’ [-Wimplicit-f
claration]
setuid(getuid()); /* getuid() returns the real uid */
^
2.9.c:20:5: warning: implicit declaration of function ‘fork’ [-Wimplicit-fun
ction-declaration]
if (fork()) { /* In the parent process */
^
2.9.c:21:1: warning: implicit declaration of function ‘close’ [-Wimplicit-fu
nction-declaration]
close (fd);
^
2.9.c:27:1: warning: implicit declaration of function ‘write’ [-Wimplicit-fu
nction-declaration]
write (fd, "Malicious Data\n", 15);
^
[09/28/20]seed@VM:~/host$ gcc 2.9.c
[09/28/20]seed@VM:~/host$ sudo chown root a.out
[09/28/20]seed@VM:~/host$ sudo chmod 4755 a.out
[09/28/20]seed@VM:~/host$ ./a.out
Cannot open /etc/zzz
[09/28/20]seed@VM:~/host$