Lab report

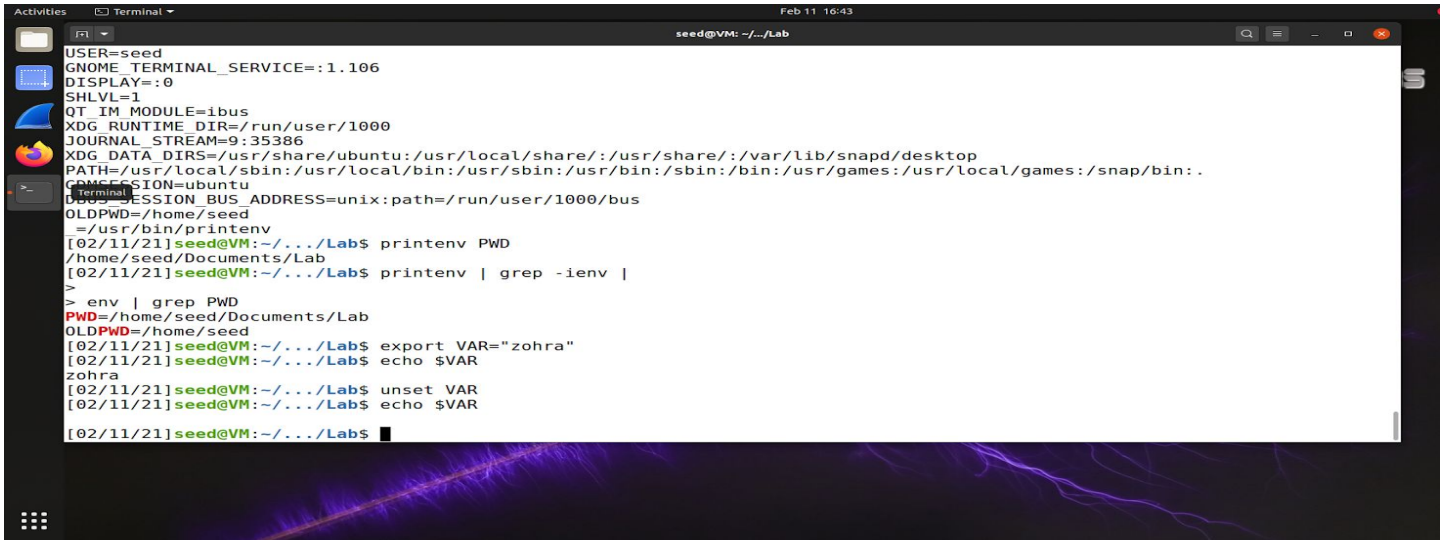
5382 Secure Programming

Assignment 1

Submitted by: Begum Fatima Zohra

UTA ID: 1001880881

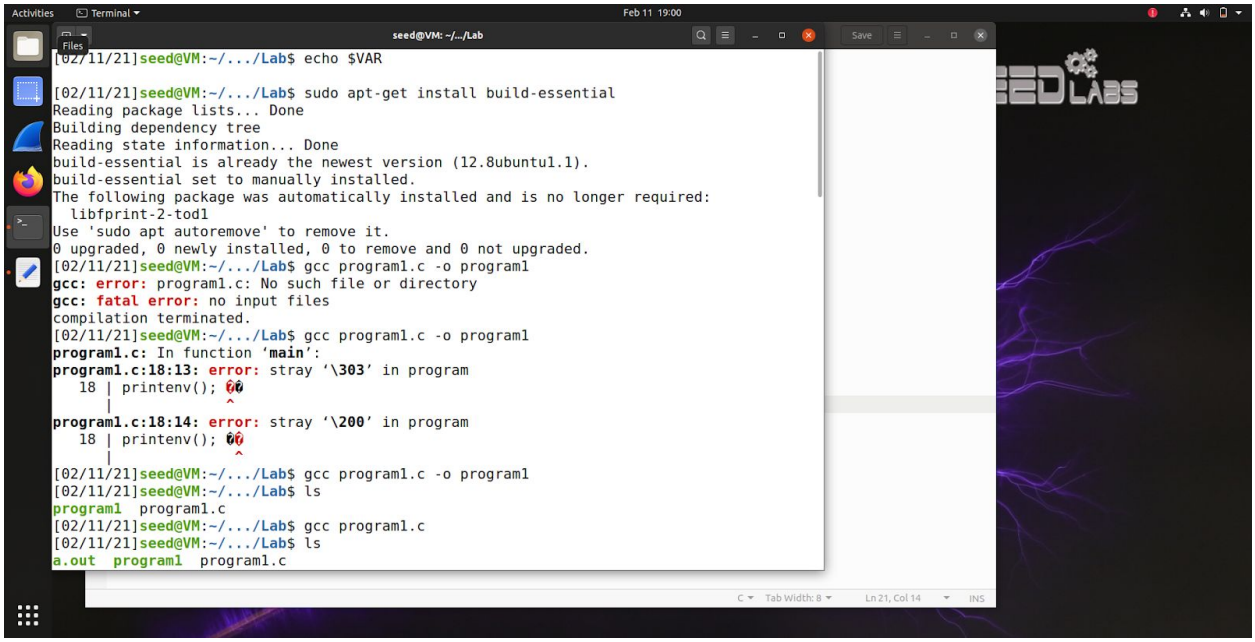
Task 1: Manipulating Environment Variables



printenv prints all the environment variables
printenv PWD prints the current PWD
env | grep PWD prints both new and old PWD

export VAR=”zohra” sets VAR value to zohra which is shown through echo $VAR
unset VAR=”zohra” removes the VAR value

Task 2: Passing Environment Variables from Parent Process to Child Process



Here, first we installed the build-essential because "build-essential" contains tools (like the gcc compiler, make tool, etc) for compiling/building software from source. So you start with (usually C) source files and create executables from them.

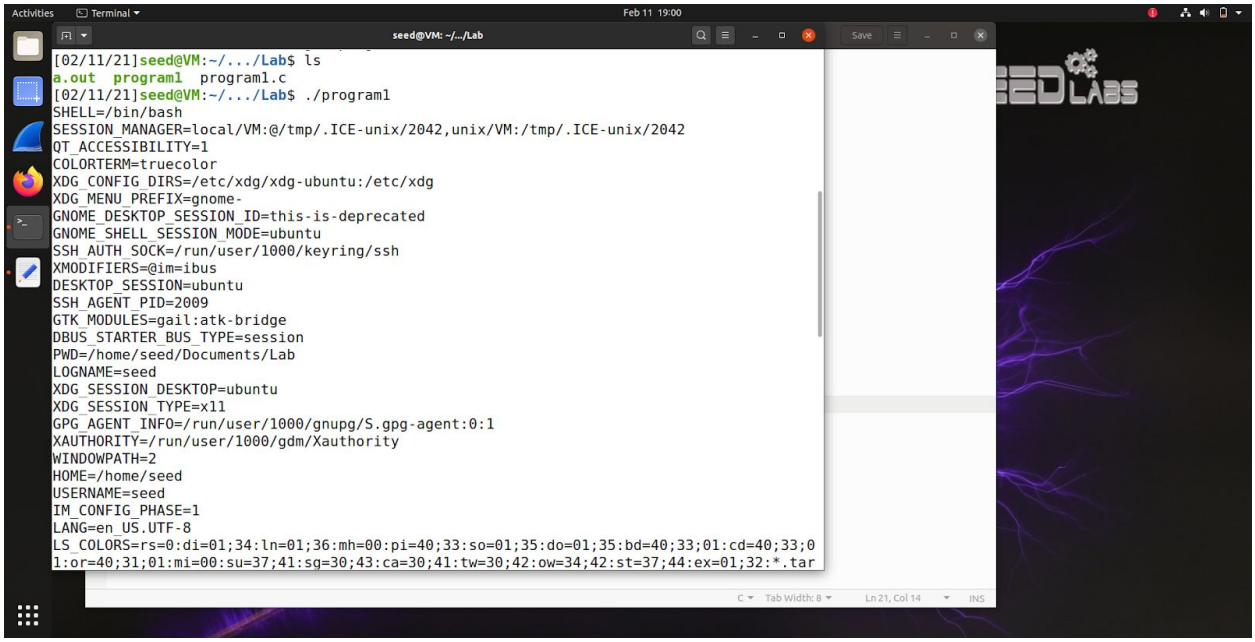
For step 1, we ran the compiled and ran the program1, which basically printed the environment variables since the case is 0.

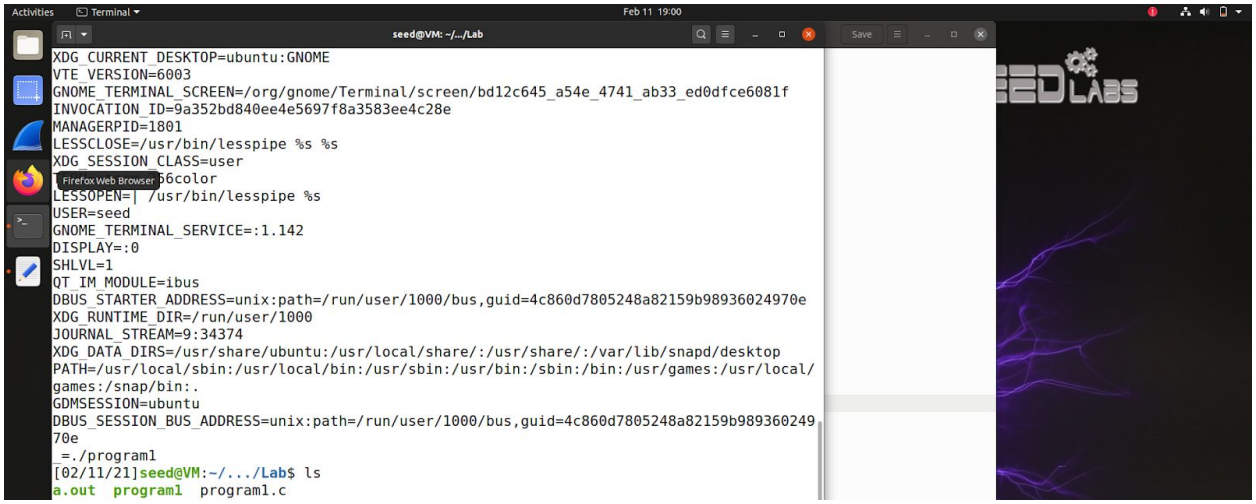
We saved the output of program1 in child(program1 > child), copied the content of program1 to p1child, and ran program1 as p1parent (parent process) because we want to separately run parent and child processes to know the diff.

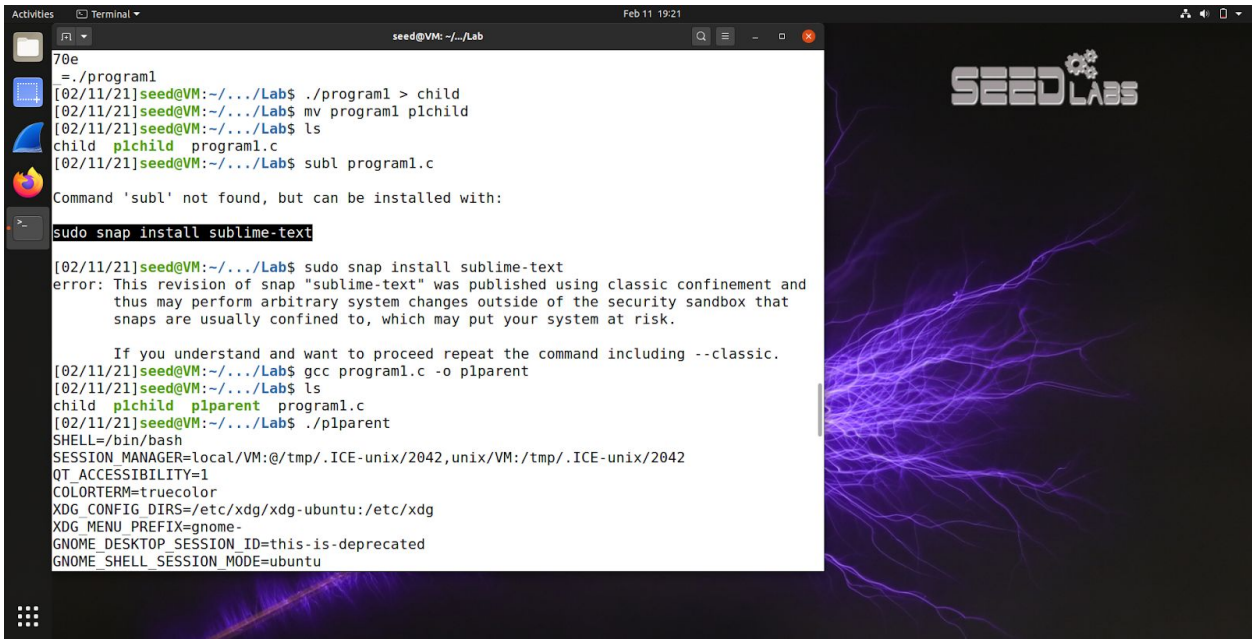
For step 2, we commented out the printenv() statement in the child process p1child, and uncomment the printenv() statement. We ran and saved the result in child. The result was the same as step 1.

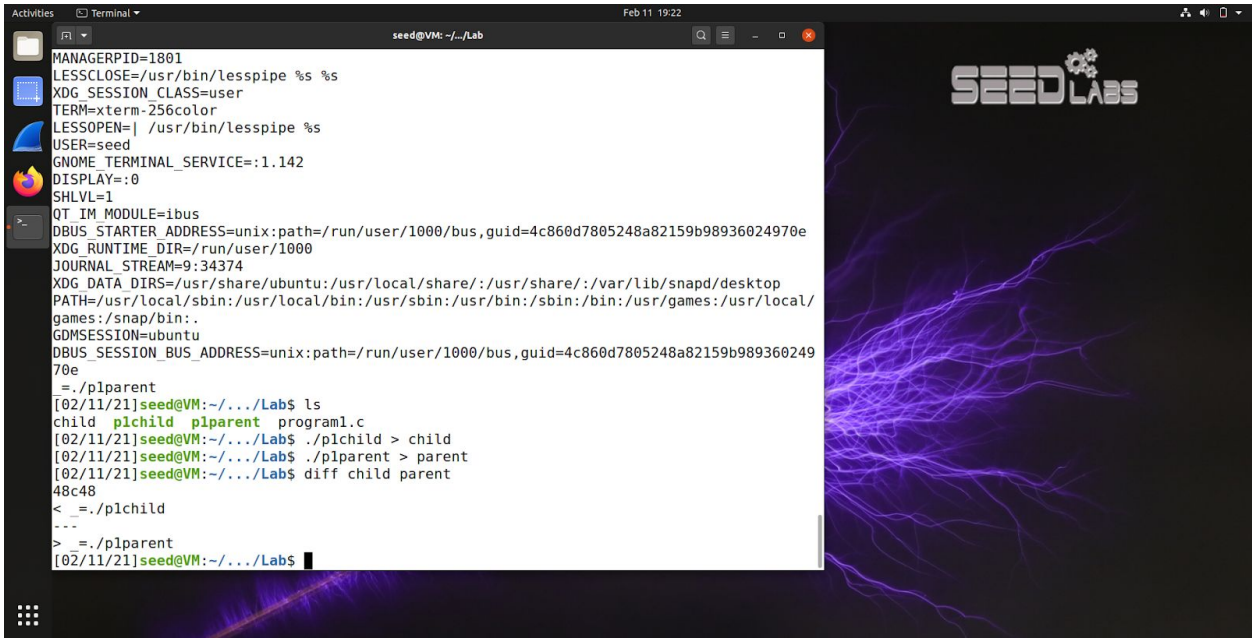
For step 3, we ran and saved the result of p1parent as parent. To know the diff we ran the following command: diff child parent.

Both of them proved to be equal.


Activities
Terminal
Feb 11 19:00
seed@VM: ~/.../Lab
Save
[02/11/21]seed@VM:~/.../Lab$ ls
a.out program1 program1.c
[02/11/21]seed@VM:~/.../Lab$ ./program1
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/2042,unix/VM:/tmp/.ICE-unix/2042
QT_ACCESSIBILITY=1
COLORTERM=truecolor
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/etc/xdg
XDG_MENU_PREFIX=gnome-
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
GNOME_SHELL_SESSION_MODE=ubuntu
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
XMODIFIERS=@im=ibus
DESKTOP_SESSION=ubuntu
SSH_AGENT_PID=2009
GTK_MODULES=gail:atk-bridge
DBUS_STARTER_BUS_TYPE=session
PWD=/home/seed/Documents/Lab
LOGNAME=seed
XDG_SESSION_DESKTOP=ubuntu
XDG_SESSION_TYPE=x11
GPG_AGENT_INFO=/run/user/1000/gnupg/S.gpg-agent:0:1
XAUTHORITY=/run/user/1000/gdm/Xauthority
WINDOWPATH=2
HOME=/home/seed
USERNAME=seed
IM_CONFIG_PHASE=1
LANG=en_US.UTF-8
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;0
1: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
C
Tab Width: 8
Ln 21, Col 14
INS


Activities
Terminal
Feb 11 19:00
seed@VM: ~/.../Lab
Save
Firefox Web Browser
XDG_CURRENT_DESKTOP=ubuntu:GNOME
VTE_VERSION=6003
GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/bd12c645_a54e_4741_ab33_ed0dfce6081f
INVOCATION_ID=9a352bd840ee4e5697f8a3583ee4c28e
MANAGERPID=1801
LESSCLOSE=/usr/bin/lesspipe %s %s
XDG_SESSION_CLASS=user
TERM=xterm-256color
LESSOPEN=| /usr/bin/lesspipe %s
USER=seed
GNOME_TERMINAL_SERVICE=:1.142
DISPLAY=:0
SHLVL=1
QT_IM_MODULE=ibus
DBUS_STARTER_ADDRESS=unix:path=/run/user/1000/bus,guid=4c860d7805248a82159b98936024970e
XDG_RUNTIME_DIR=/run/user/1000
JOURNAL_STREAM=9:34374
XDG_DATA_DIRS=/usr/share/ubuntu:/usr/local/share/:/usr/share/:/var/lib/snapd/desktop
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin:.
GDMSESSION=ubuntu
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus,guid=4c860d7805248a82159b98936024970e
_=./program1
[02/11/21]seed@VM:~/.../Lab$ ls
a.out program1 program1.c


Activities
Terminal
Feb 11 19:21
seed@VM: ~/.../Lab
70e
_=./program1
[02/11/21]seed@VM:~/.../Lab$ ./program1 > child
[02/11/21]seed@VM:~/.../Lab$ mv program1 p1child
[02/11/21]seed@VM:~/.../Lab$ ls
child p1child program1.c
[02/11/21]seed@VM:~/.../Lab$ subl program1.c
Command 'subl' not found, but can be installed with:
sudo snap install sublime-text
[02/11/21]seed@VM:~/.../Lab$ sudo snap install sublime-text
error: This revision of snap "sublime-text" was published using classic confinement and
thus may perform arbitrary system changes outside of the security sandbox that
snaps are usually confined to, which may put your system at risk.
If you understand and want to proceed repeat the command including --classic.
[02/11/21]seed@VM:~/.../Lab$ gcc program1.c -o p1parent
[02/11/21]seed@VM:~/.../Lab$ ls
child p1child p1parent program1.c
[02/11/21]seed@VM:~/.../Lab$ ./p1parent
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/2042,unix/VM:/tmp/.ICE-unix/2042
QT_ACCESSIBILITY=1
COLORTERM=truecolor
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/etc/xdg
XDG_MENU_PREFIX=gnome-
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
GNOME_SHELL_SESSION_MODE=ubuntu

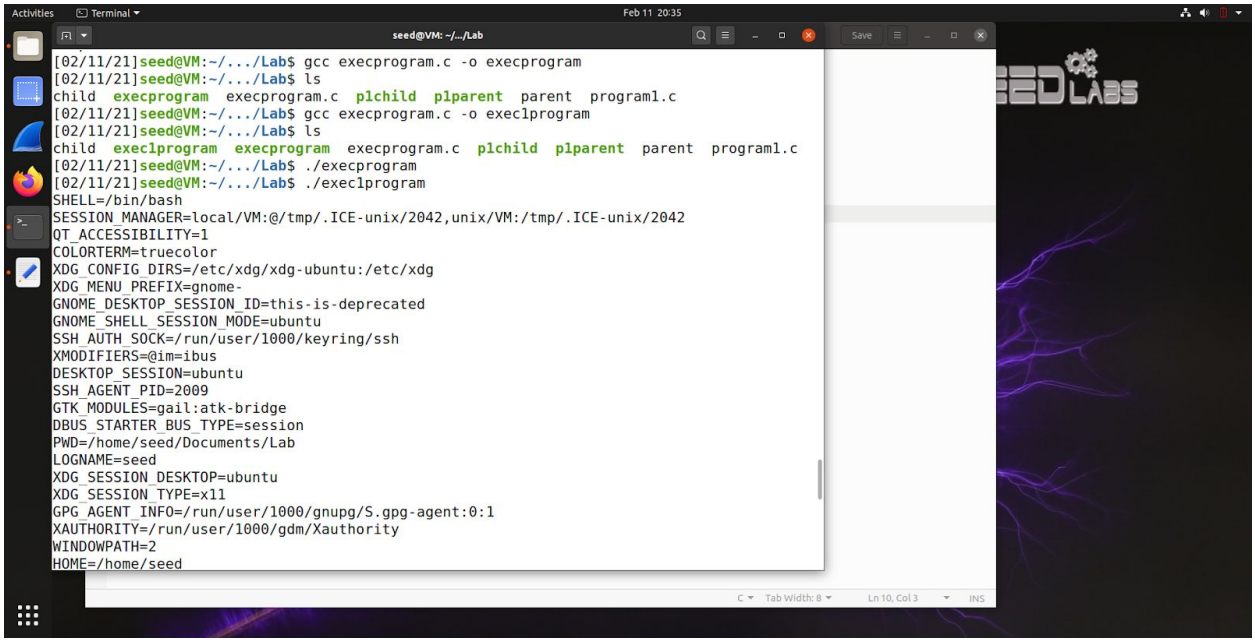


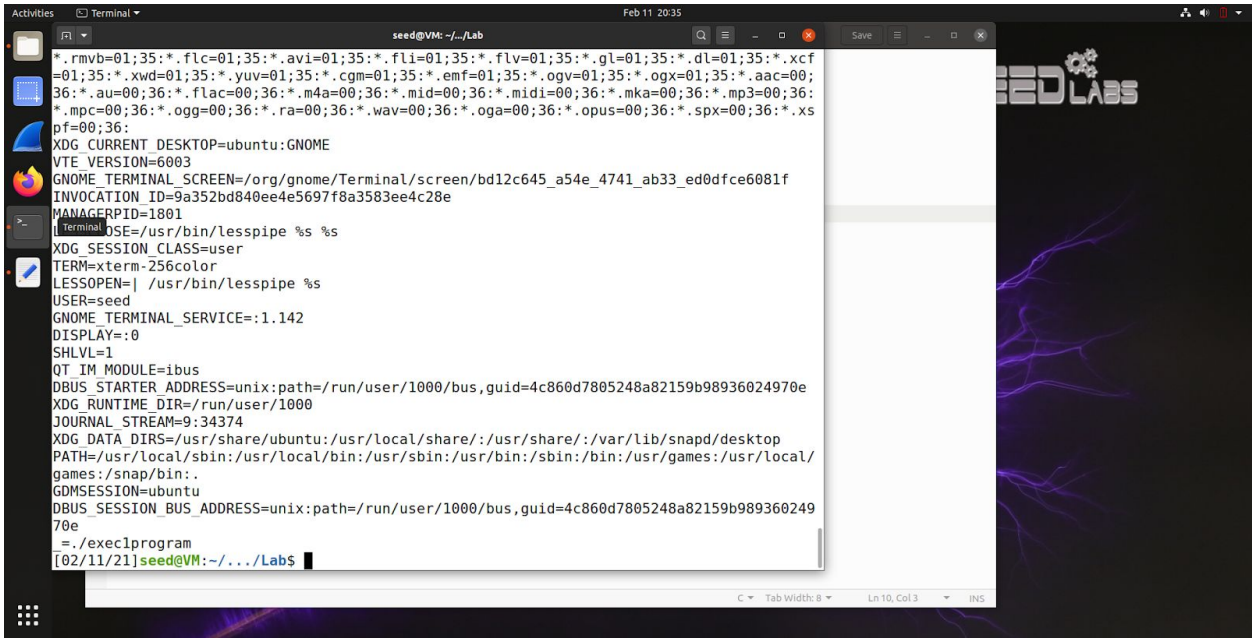
Task 3: Environment Variables and execve()

Step 1: compiled the program execprogram.c as execprogram. It did not print the environment variables of the current process. Reason: argv[1] which is the second parameter of execve() is set to NULL.

Step 2: compiled the program execprogram.c as exec1program. It did print the environment variables of the current process. Reason: argv[1] which is the second parameter of execve() is set to environ → execve("/usr/bin/env", argv, environ);

Step3: Conclusion→ function execve() overwrites

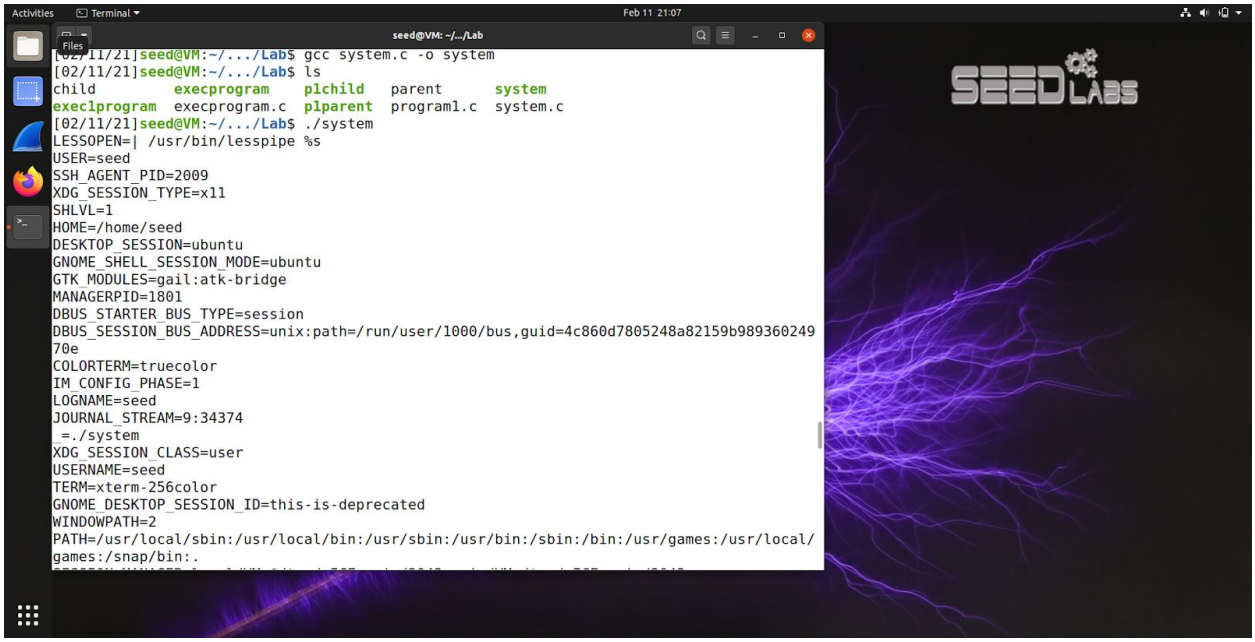

Activities
Terminal
Feb 11 20:35
seed@VM: ~/.../Lab
Save
[02/11/21]seed@VM:~/.../Lab$ gcc execprogram.c -o execprogram
[02/11/21]seed@VM:~/.../Lab$ ls
child execprogram execprogram.c p1child p1parent parent program1.c
[02/11/21]seed@VM:~/.../Lab$ gcc execprogram.c -o exec1program
[02/11/21]seed@VM:~/.../Lab$ ls
child exec1program execprogram execprogram.c p1child p1parent parent program1.c
[02/11/21]seed@VM:~/.../Lab$ ./execprogram
[02/11/21]seed@VM:~/.../Lab$ ./exec1program
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/2042,unix/VM:/tmp/.ICE-unix/2042
QT_ACCESSIBILITY=1
COLORTERM=truecolor
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/etc/xdg
XDG_MENU_PREFIX=gnome-
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
GNOME_SHELL_SESSION_MODE=ubuntu
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
XMODIFIERS=@im=ibus
DESKTOP_SESSION=ubuntu
SSH_AGENT_PID=2009
GTK_MODULES=gail:atk-bridge
DBUS_STARTER_BUS_TYPE=session
PWD=/home/seed/Documents/Lab
LOGNAME=seed
XDG_SESSION_DESKTOP=ubuntu
XDG_SESSION_TYPE=x11
GPG_AGENT_INFO=/run/user/1000/gnupg/S.gpg-agent:0:1
XAUTHORITY=/run/user/1000/gdm/Xauthority
WINDOWPATH=2
HOME=/home/seed
C
Tab Width: 8
Ln 10, Col 3
INS

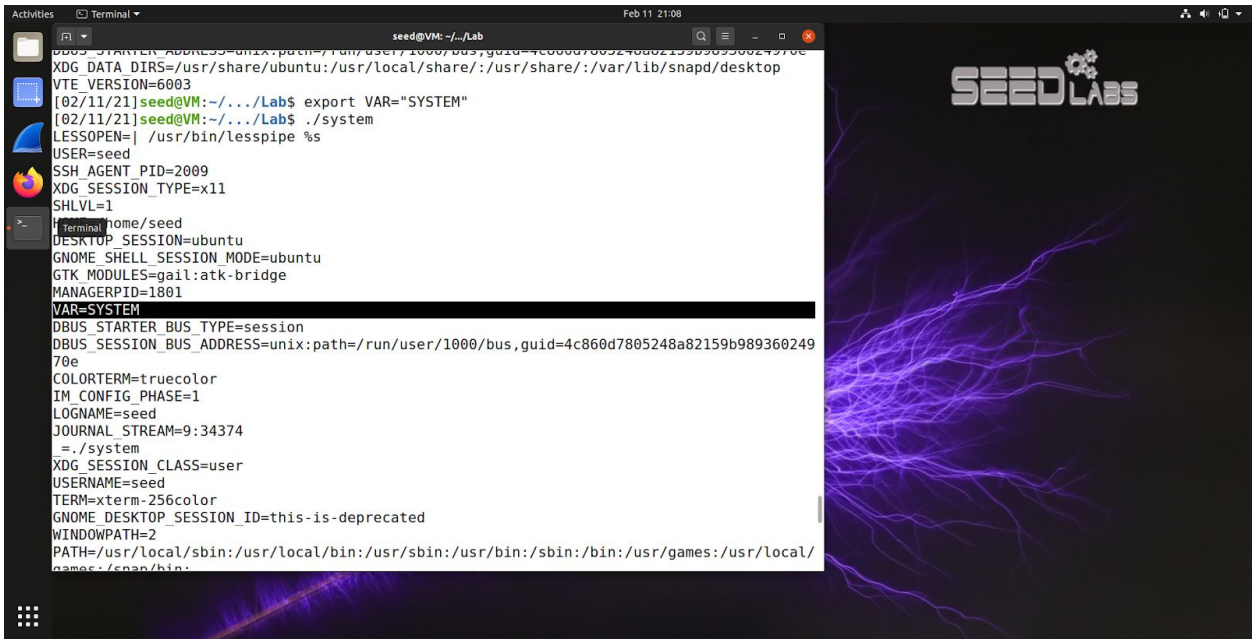

Activities
Terminal
Feb 11 20:35
seed@VM: ~/.../Lab
Save
.rmvb=01;35:.flc=01;35:*.avi=01;35:*.fli=01;35:*.flv=01;35:*.gl=01;35:*.dl=01;35:*.xcf
=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm=01;35:*.emf=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=00;
36:*.au=00;36:*.flac=00;36:*.m4a=00;36:*.mid=00;36:*.midi=00;36:*.mka=00;36:*.mp3=00;36:
.mpc=00;36:.ogg=00;36:*.ra=00;36:*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xs
pf=00;36:
XDG_CURRENT_DESKTOP=ubuntu:GNOME
VTE_VERSION=6003
GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/bd12c645_a54e_4741_ab33_ed0dfce6081f
INVOCATION_ID=9a352bd840ee4e5697f8a3583ee4c28e
MANAGERPID=1801
LESSCLOSE=/usr/bin/lesspipe %s %s
XDG_SESSION_CLASS=user
TERM=xterm-256color
LESSOPEN=| /usr/bin/lesspipe %s
USER=seed
GNOME_TERMINAL_SERVICE=:1.142
DISPLAY=:0
SHLVL=1
QT_IM_MODULE=ibus
DBUS_STARTER_ADDRESS=unix:path=/run/user/1000/bus,guid=4c860d7805248a82159b98936024970e
XDG_RUNTIME_DIR=/run/user/1000
JOURNAL_STREAM=9:34374
XDG_DATA_DIRS=/usr/share/ubuntu:/usr/local/share/:/usr/share/:/var/lib/snapd/desktop
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/
games:/snap/bin:.
GDMSESSION=ubuntu
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus,guid=4c860d7805248a82159b989360249
70e
_=./exec1program
[02/11/21]seed@VM:~/.../Lab$
Terminal
C
Tab Width: 8
Ln 10, Col 3
INS

Task 4: Environment Variables and system()

Through Task 3, we got to know that execve() is a safe way to run the program. It directly executes the program. But system() is not safe since it executes /bin/sh -c command. This is a vulnerable way.

To identify this behavior, we first compiled the program system.c and ran it. All the environment variables are shown in the terminal. Then, we set VAR=”system” and ran ./system program. As you could see VAR=system is visible in the output. Therefore, using system(), the environment variables of the calling process is passed to the new program





Task 5: Environment Variable and Set-UID Programs

Step 1: We compiled and ran setuid.c program. All the environment variables in the current process were printed in the terminal.

Step 2: Changed setuid program's ownership to root, and make it a Set-UID program.

./setuid grep | -i PATH

The inherited PATH is shown.

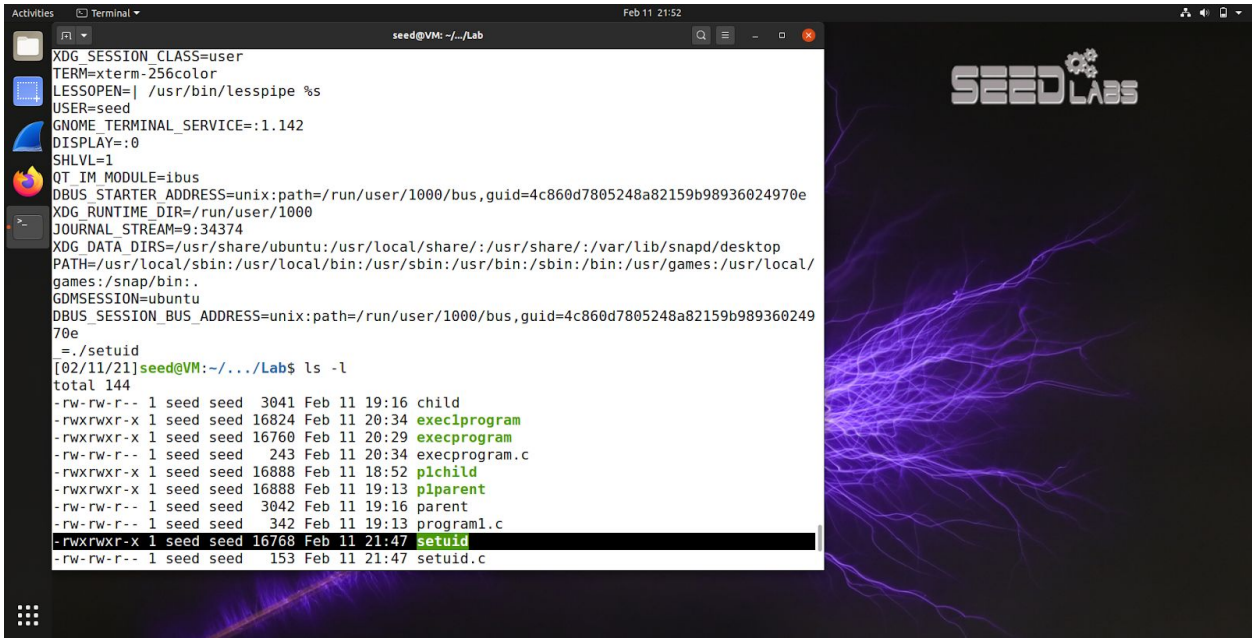
./setuid grep | -i LD_LIBRARY_PATH
NO LD_LIBRARY_PATH is inherited

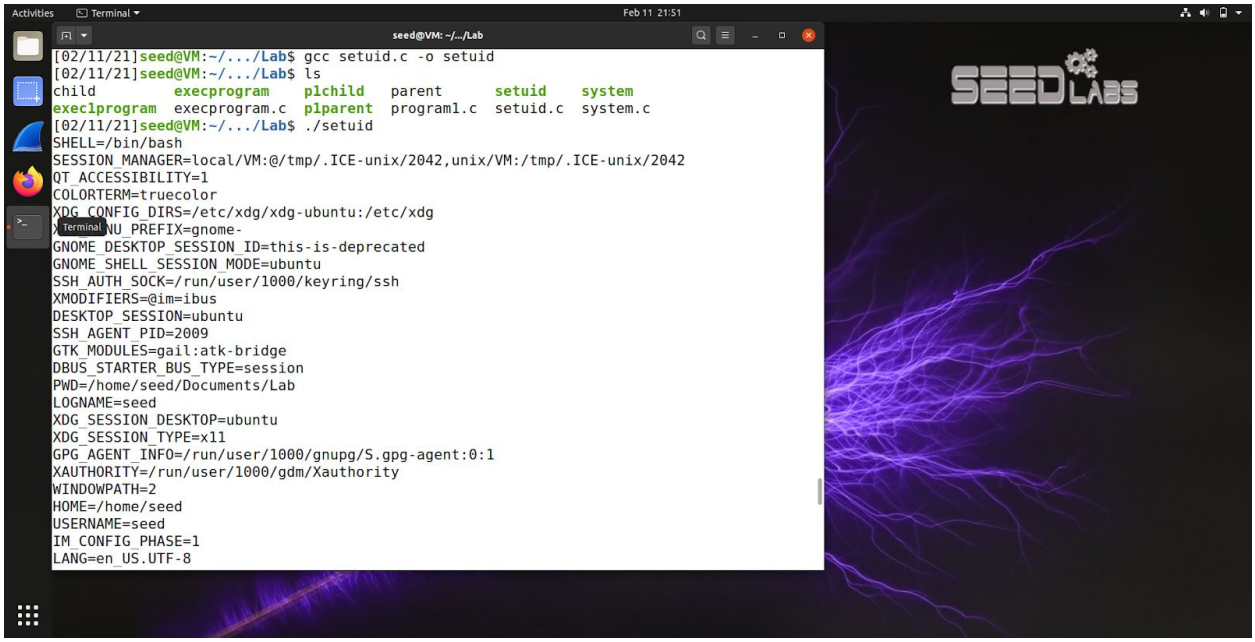
./setuid grep | -i PROGRAM

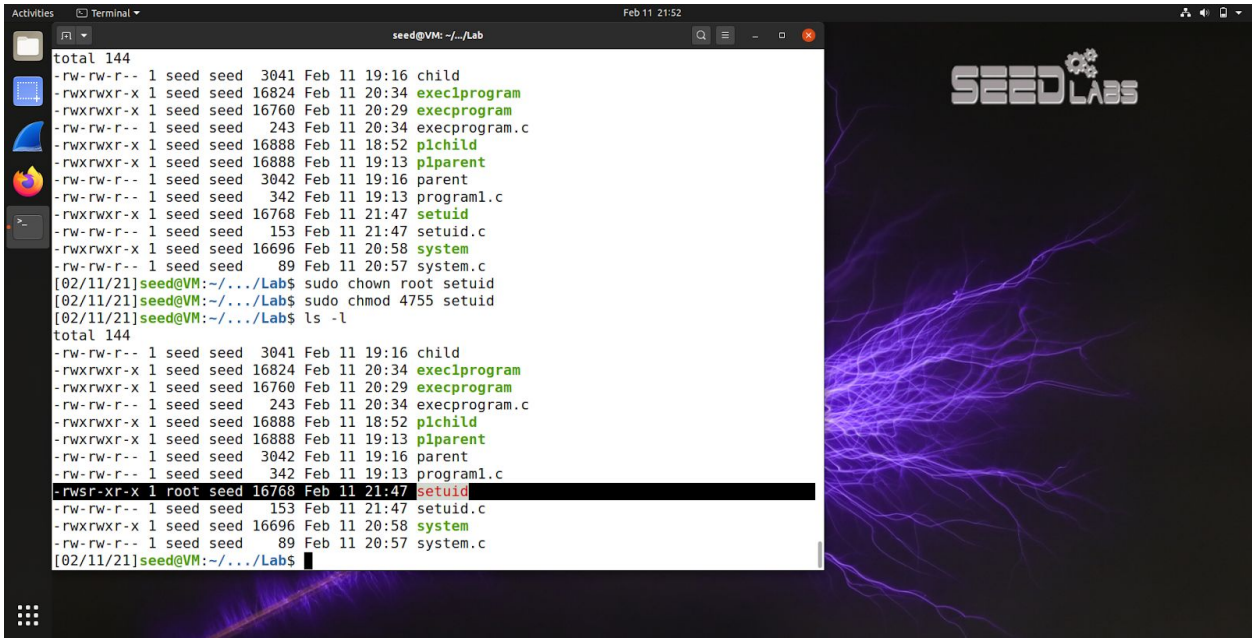
NO PROGRAM environment variable(s) is inherited

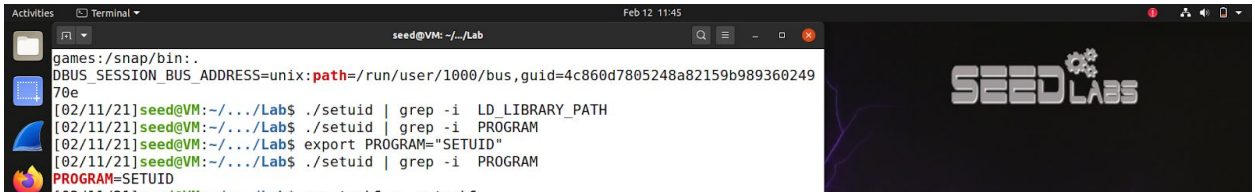
So, we executed the commands → export PROGRAM=”SETUID”
./setuid grep | -i PROGRAM
PROGRAM was successfully set and inherited.

User defined variable PROGRAM was inherited after using the export command.
But, LD_LIBRARY_PATH was now inherited by the child process since it is a built-in environment variable in the user’s shell process. A child process cannot change shell's environment.


Activities
Terminal
Feb 11 21:52
seed@VM: ~/.../Lab
XDG_SESSION_CLASS=user
TERM=xterm-256color
LESSOPEN=| /usr/bin/lesspipe %s
USER=seed
GNOME_TERMINAL_SERVICE=:1.142
DISPLAY=:0
SHLVL=1
QT_IM_MODULE=ibus
DBUS_STARTER_ADDRESS=unix:path=/run/user/1000/bus,guid=4c860d7805248a82159b98936024970e
XDG_RUNTIME_DIR=/run/user/1000
JOURNAL_STREAM=9:34374
XDG_DATA_DIRS=/usr/share/ubuntu:/usr/local/share/:/usr/share/:/var/lib/snapd/desktop
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin:.
GDMSESSION=ubuntu
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus,guid=4c860d7805248a82159b98936024970e
_=./setuid
[02/11/21]seed@VM:~/.../Lab$ ls -l
total 144
-rw-rw-r-- 1 seed seed 3041 Feb 11 19:16 child
-rwxrwxr-x 1 seed seed 16824 Feb 11 20:34 execlprogram
-rwxrwxr-x 1 seed seed 16760 Feb 11 20:29 execprogram
-rw-rw-r-- 1 seed seed   243 Feb 11 20:34 execprogram.c
-rwxrwxr-x 1 seed seed 16888 Feb 11 18:52 plchild
-rwxrwxr-x 1 seed seed 16888 Feb 11 19:13 plparent
-rw-rw-r-- 1 seed seed 3042 Feb 11 19:16 parent
-rw-rw-r-- 1 seed seed   342 Feb 11 19:13 program1.c
-rwxrwxr-x 1 seed seed 16768 Feb 11 21:47 setuid
-rw-rw-r-- 1 seed seed   153 Feb 11 21:47 setuid.c


Activities
Terminal
Feb 11 21:51
seed@VM: ~/.../Lab
[02/11/21]seed@VM:~/.../Lab$ gcc setuid.c -o setuid
[02/11/21]seed@VM:~/.../Lab$ ls
child execprogram plchild parent setuid system
execlprogram execprogram.c plparent program1.c setuid.c system.c
[02/11/21]seed@VM:~/.../Lab$ ./setuid
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/2042,unix/VM:/tmp/.ICE-unix/2042
QT_ACCESSIBILITY=1
COLORTERM=truecolor
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/etc/xdg
Terminal
NU_PREFIX=gnome-
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
GNOME_SHELL_SESSION_MODE=ubuntu
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
XMODIFIERS=@im=ibus
DESKTOP_SESSION=ubuntu
SSH_AGENT_PID=2009
GTK_MODULES=gail:atk-bridge
DBUS_STARTER_BUS_TYPE=session
PWD=/home/seed/Documents/Lab
LOGNAME=seed
XDG_SESSION_DESKTOP=ubuntu
XDG_SESSION_TYPE=x11
GPG_AGENT_INFO=/run/user/1000/gnupg/S.gpg-agent:0:1
XAUTHORITY=/run/user/1000/gdm/Xauthority
WINDOWPATH=2
HOME=/home/seed
USERNAME=seed
IM_CONFIG_PHASE=1
LANG=en_US.UTF-8

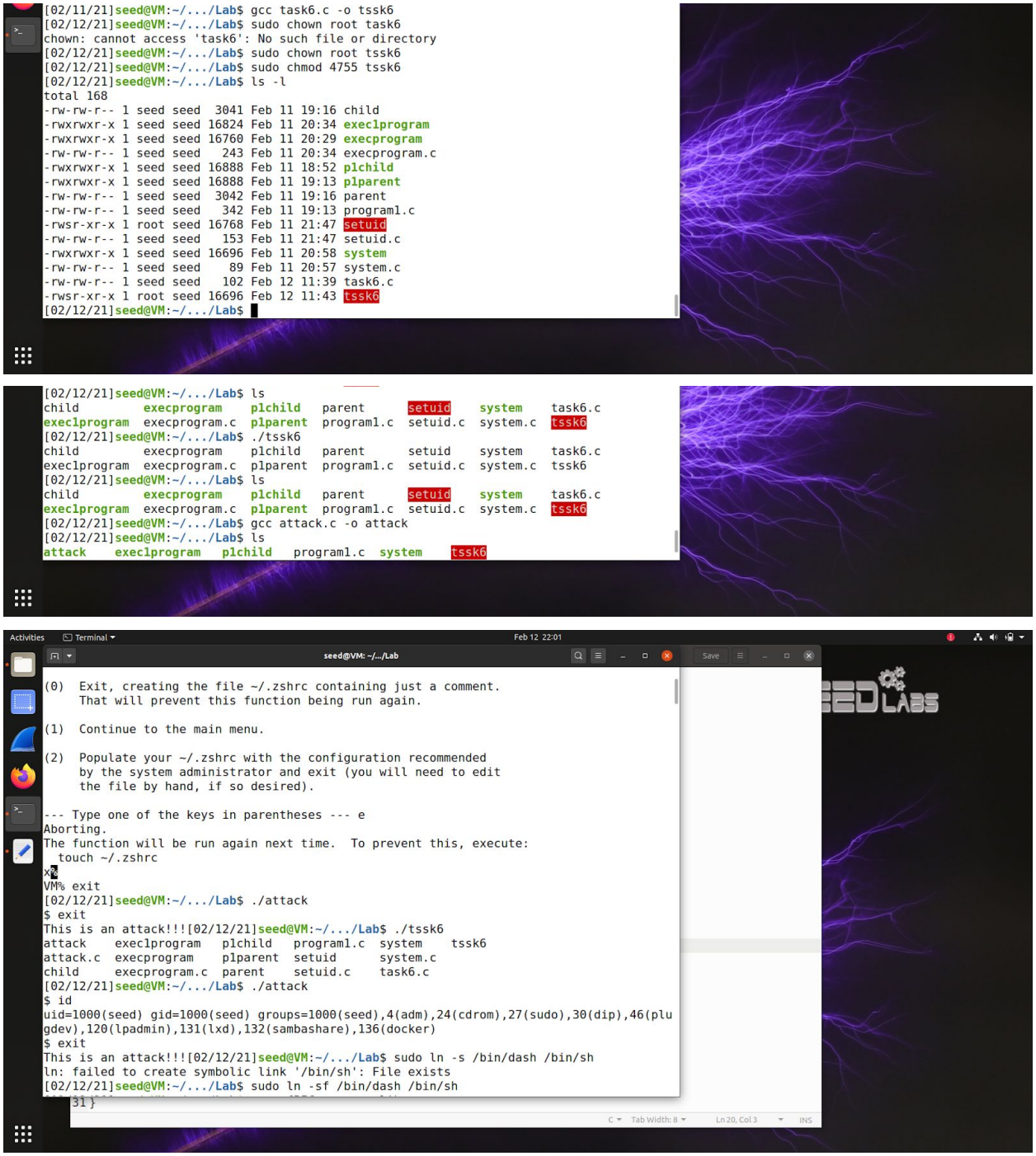




Task 6: The PATH Environment Variable and Set-UID Programs

Compiled task6.c program. Changed its owner to root. Ran ./tssk6 as a SET_UID program. We then created a malicious program attack.c which does not have a root ownership. It has all the contents of the task6.c program plus an extra line “this is an attack”

We removed the current link to dash through sudo rm /bin/sh
Then linked to the zsh which has no counter measures.
We ran ./attack our attack works without such a countermeasure.



Task 7: The LD_PRELOAD Environment Variable and Set-UID Programs

Step 1: Created a program, and compiled it as `mylib.c`.

set the LD_PRELOAD environment variable:

Finally, compiled the program `myprog` in the same directory as `libmylib.so.1.0.1`

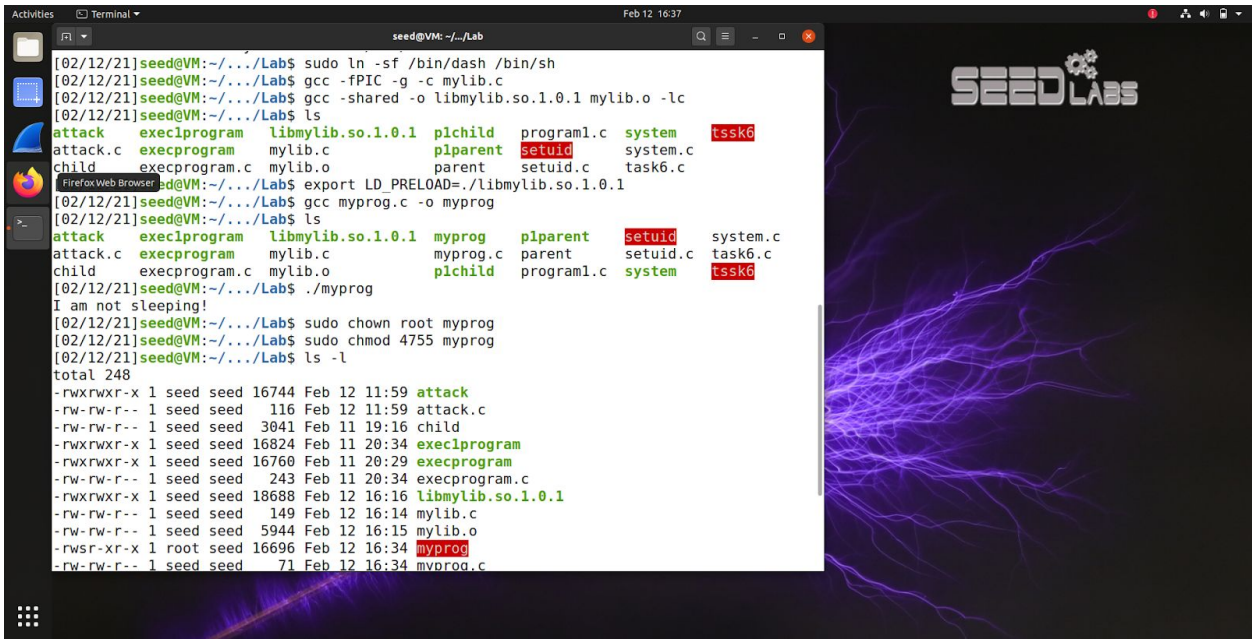
Step 2: Ran the program as a normal user. Output “I am not sleeping!” came after 1 second.

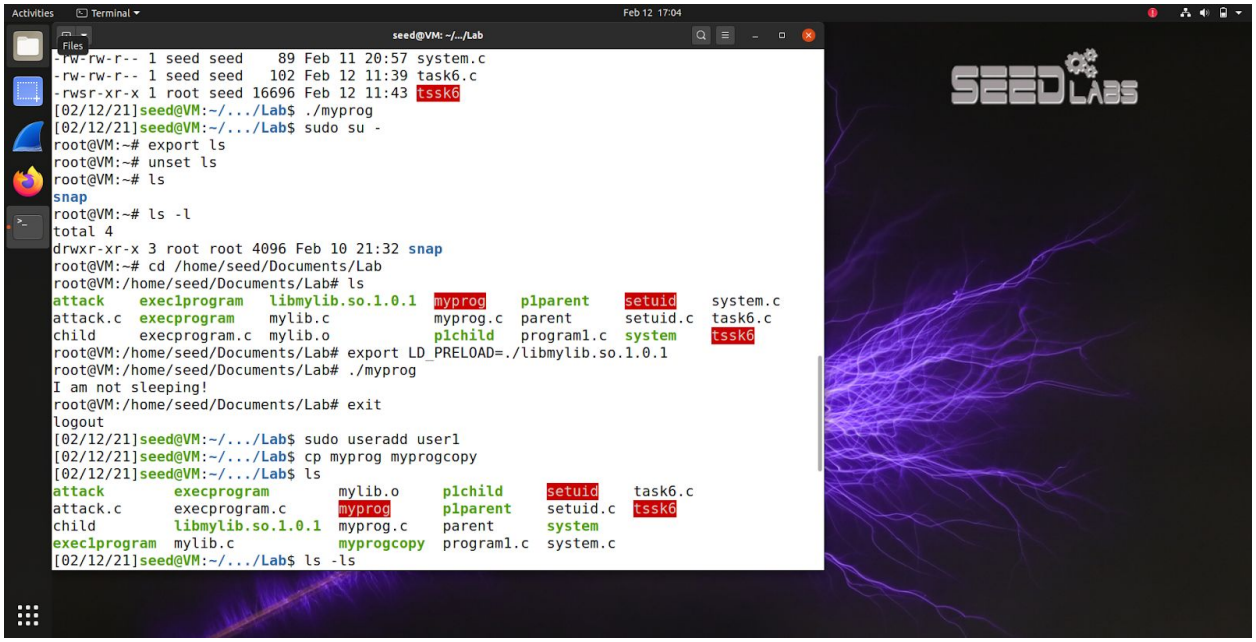
Made myprog a Set-UID root program, and ran it as a normal user.
Here it ignored the LD_PRELOAD environment variable and used the system's default `sleep()` function. So `sleep()` function did not override.

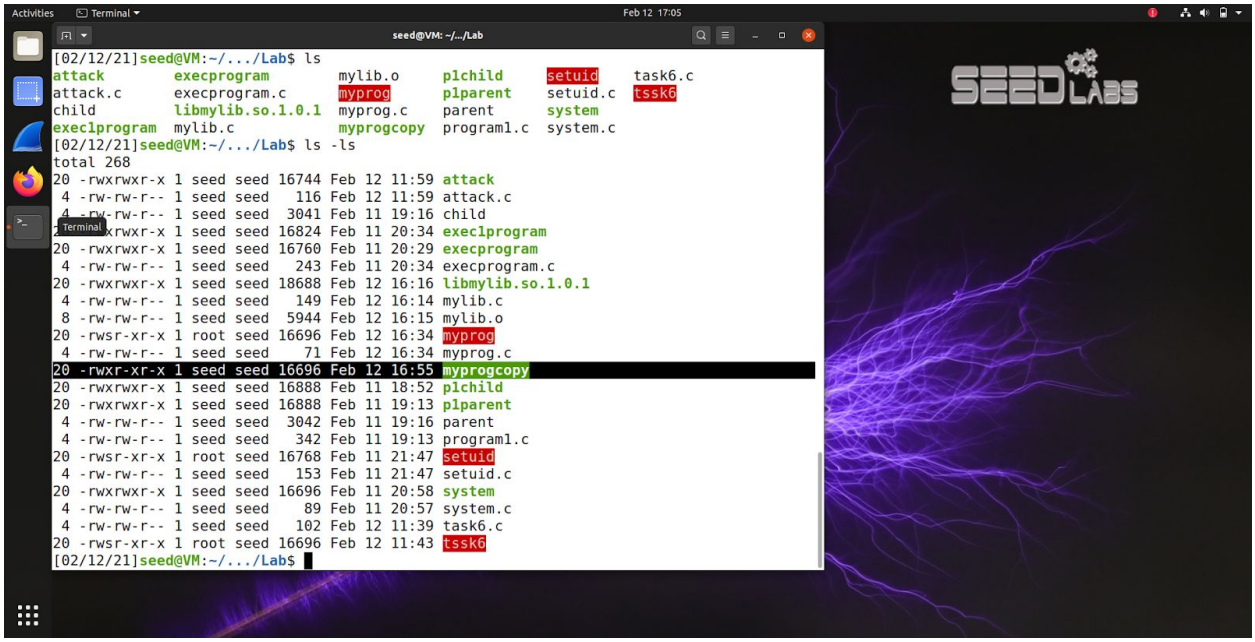
Made myprog a Set-UID root program, and ran it in the root account.
Here, it used the LD_PRELOAD environment variable and override `sleep()` function.

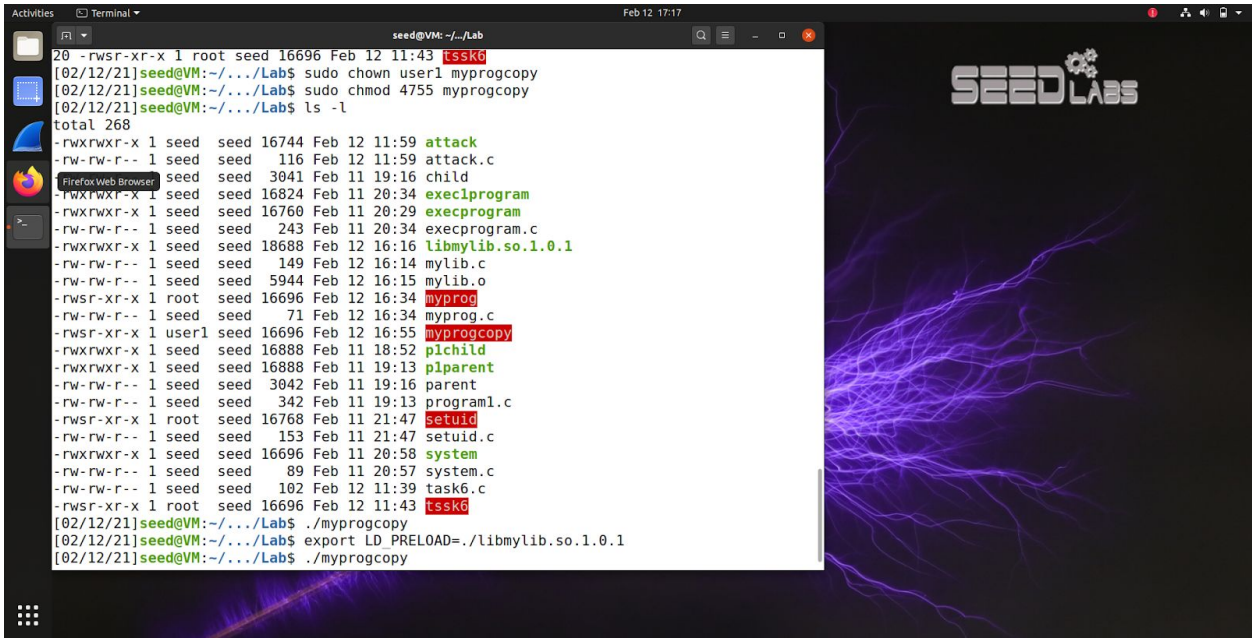
Made myprog a Set-UID user1 program (i.e., the owner is user1, which is another user account), and run it as a different user (not-root user).
Here, it did not override `sleep()` function.

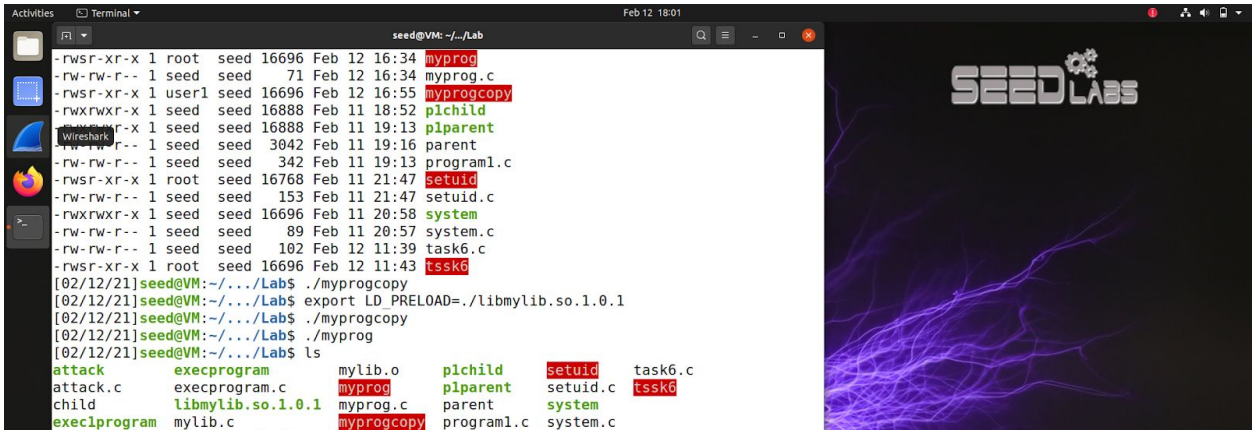
Step 3: Conclusions: a user can run the program created by himself, `LD_PRELOAD` environment variable can be used and `sleep()` function can be overridden.




Activities
Terminal
Feb 12 17:04
Files
seed@VM: ~/.../Lab
-rw-rw-r-- 1 seed seed 89 Feb 11 20:57 system.c
-rw-rw-r-- 1 seed seed 102 Feb 12 11:39 task6.c
-rwsr-xr-x 1 root seed 16696 Feb 12 11:43 tssk6
[02/12/21]seed@VM:~/.../Lab$ ./myprog
[02/12/21]seed@VM:~/.../Lab$ sudo su -
root@VM:~# export ls
root@VM:~# unset ls
root@VM:~# ls
snap
root@VM:~# ls -l
total 4
drwxr-xr-x 3 root root 4096 Feb 10 21:32 snap
root@VM:~# cd /home/seed/Documents/Lab
root@VM:/home/seed/Documents/Lab# ls
attack execlprogram libmylib.so.1.0.1 myprog p1parent setuid system.c
attack.c execprogram mylib.c myprog.c parent setuid.c task6.c
child execprogram.c mylib.o p1child program1.c system tssk6
root@VM:/home/seed/Documents/Lab# export LD_PRELOAD=./libmylib.so.1.0.1
root@VM:/home/seed/Documents/Lab# ./myprog
I am not sleeping!
root@VM:/home/seed/Documents/Lab# exit
logout
[02/12/21]seed@VM:~/.../Lab$ sudo useradd user1
[02/12/21]seed@VM:~/.../Lab$ cp myprog myprogcopy
[02/12/21]seed@VM:~/.../Lab$ ls
attack execprogram mylib.o p1child setuid task6.c
attack.c execprogram.c myprog p1parent setuid.c tssk6
child libmylib.so.1.0.1 myprog.c parent system
execlprogram mylib.c myprogcopy program1.c system.c
[02/12/21]seed@VM:~/.../Lab$ ls -ls


Activities
Terminal
Feb 12 17:05
seed@VM: ~/.../Lab
[02/12/21]seed@VM:~/.../Lab$ ls
attack execprogram mylib.o p1child setuid task6.c
attack.c execprogram.c myprog p1parent setuid.c tssk6
child libmylib.so.1.0.1 myprog.c parent system
exec1program mylib.c myprogcopy program1.c system.c
[02/12/21]seed@VM:~/.../Lab$ ls -ls
total 268
20 -rwxrwxr-x 1 seed seed 16744 Feb 12 11:59 attack
4 -rw-rw-r-- 1 seed seed 116 Feb 12 11:59 attack.c
4 -rw-rw-r-- 1 seed seed 3041 Feb 11 19:16 child
Terminal
20 -rwxrwxr-x 1 seed seed 16824 Feb 11 20:34 exec1program
20 -rwxrwxr-x 1 seed seed 16760 Feb 11 20:29 execprogram
4 -rw-rw-r-- 1 seed seed 243 Feb 11 20:34 execprogram.c
20 -rwxrwxr-x 1 seed seed 18688 Feb 12 16:16 libmylib.so.1.0.1
4 -rw-rw-r-- 1 seed seed 149 Feb 12 16:14 mylib.c
8 -rw-rw-r-- 1 seed seed 5944 Feb 12 16:15 mylib.o
20 -rwsr-xr-x 1 root seed 16696 Feb 12 16:34 myprog
4 -rw-rw-r-- 1 seed seed 71 Feb 12 16:34 myprog.c
20 -rwxr-xr-x 1 seed seed 16696 Feb 12 16:55 myprogcopy
20 -rwxrwxr-x 1 seed seed 16888 Feb 11 18:52 p1child
20 -rwxrwxr-x 1 seed seed 16888 Feb 11 19:13 p1parent
4 -rw-rw-r-- 1 seed seed 3042 Feb 11 19:16 parent
4 -rw-rw-r-- 1 seed seed 342 Feb 11 19:13 program1.c
20 -rwsr-xr-x 1 root seed 16768 Feb 11 21:47 setuid
4 -rw-rw-r-- 1 seed seed 153 Feb 11 21:47 setuid.c
20 -rwxrwxr-x 1 seed seed 16696 Feb 11 20:58 system
4 -rw-rw-r-- 1 seed seed 89 Feb 11 20:57 system.c
4 -rw-rw-r-- 1 seed seed 102 Feb 12 11:39 task6.c
20 -rwsr-xr-x 1 root seed 16696 Feb 12 11:43 tssk6
[02/12/21]seed@VM:~/.../Lab$
SEED LABS


Activities
Terminal
Feb 12 17:17
seed@VM: ~/.../Lab
20 -rwsr-xr-x 1 root seed 16696 Feb 12 11:43 tssk6
[02/12/21]seed@VM:~/.../Lab$ sudo chown user1 myprogcopy
[02/12/21]seed@VM:~/.../Lab$ sudo chmod 4755 myprogcopy
[02/12/21]seed@VM:~/.../Lab$ ls -l
total 268
-rwxrwxr-x 1 seed seed 16744 Feb 12 11:59 attack
-rw-rw-r-- 1 seed seed 116 Feb 12 11:59 attack.c
-rw-rw-r-- 1 seed seed 3041 Feb 11 19:16 child
Firefox Web Browser
-rwxrwxr-x 1 seed seed 16824 Feb 11 20:34 exec1program
-rwxrwxr-x 1 seed seed 16760 Feb 11 20:29 execprogram
-rw-rw-r-- 1 seed seed 243 Feb 11 20:34 execprogram.c
-rwxrwxr-x 1 seed seed 18688 Feb 12 16:16 libmylib.so.1.0.1
-rw-rw-r-- 1 seed seed 149 Feb 12 16:14 mylib.c
-rw-rw-r-- 1 seed seed 5944 Feb 12 16:15 mylib.o
-rwsr-xr-x 1 root seed 16696 Feb 12 16:34 myprog
-rw-rw-r-- 1 seed seed 71 Feb 12 16:34 myprog.c
-rwsr-xr-x 1 user1 seed 16696 Feb 12 16:55 myprogcopy
-rwxrwxr-x 1 seed seed 16888 Feb 11 18:52 p1child
-rwxrwxr-x 1 seed seed 16888 Feb 11 19:13 p1parent
-rw-rw-r-- 1 seed seed 3042 Feb 11 19:16 parent
-rw-rw-r-- 1 seed seed 342 Feb 11 19:13 program1.c
-rwsr-xr-x 1 root seed 16768 Feb 11 21:47 setuid
-rw-rw-r-- 1 seed seed 153 Feb 11 21:47 setuid.c
-rwxrwxr-x 1 seed seed 16696 Feb 11 20:58 system
-rw-rw-r-- 1 seed seed 89 Feb 11 20:57 system.c
-rw-rw-r-- 1 seed seed 102 Feb 12 11:39 task6.c
-rwsr-xr-x 1 root seed 16696 Feb 12 11:43 tssk6
[02/12/21]seed@VM:~/.../Lab$ ./myprogcopy
[02/12/21]seed@VM:~/.../Lab$ export LD_PRELOAD=./libmylib.so.1.0.1
[02/12/21]seed@VM:~/.../Lab$ ./myprogcopy
SEED LABS



Task 8: Invoking External Programs Using system() versus execve()

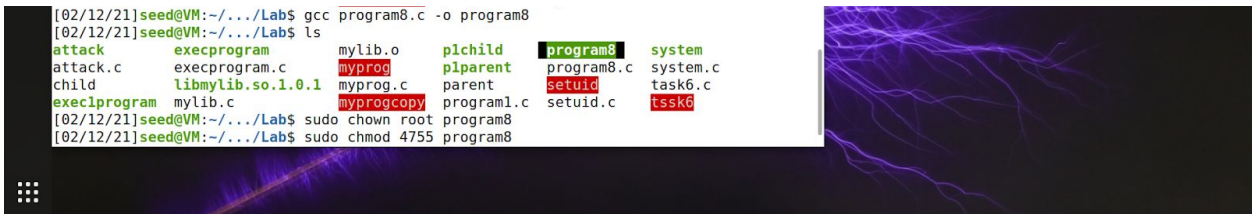
Step 1: Compiled the program as program8.c and changed its ownership to root.

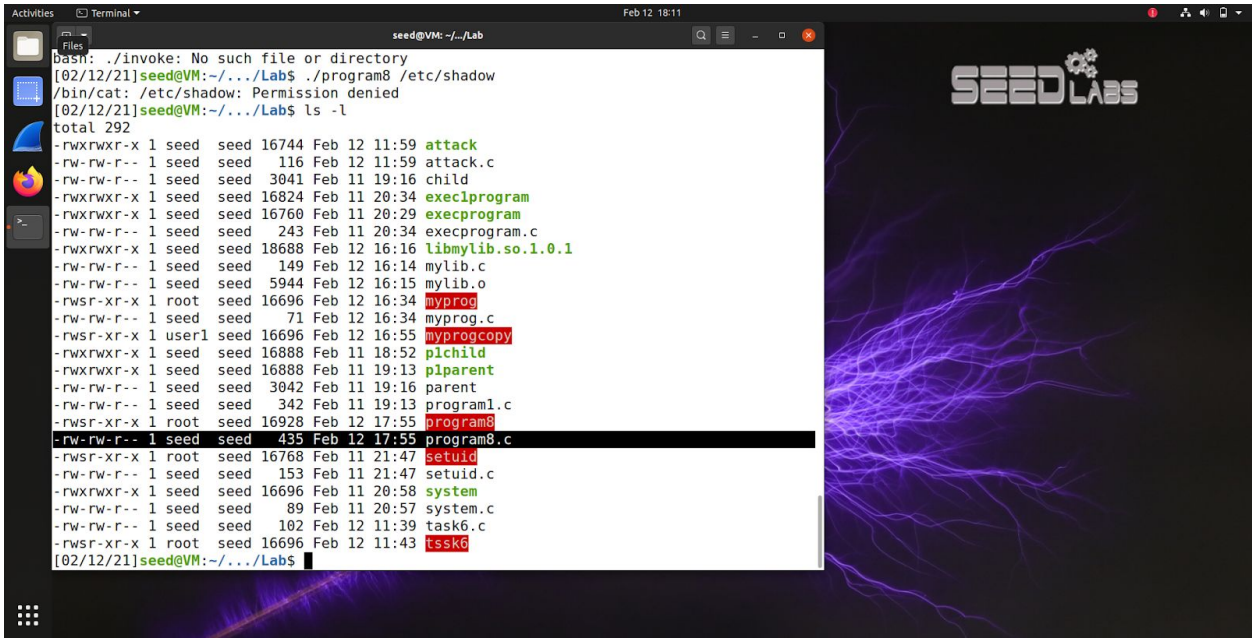
/etc/shadow is executed through /program8. Permission denied.
We could not access the secured file because we are in dash.

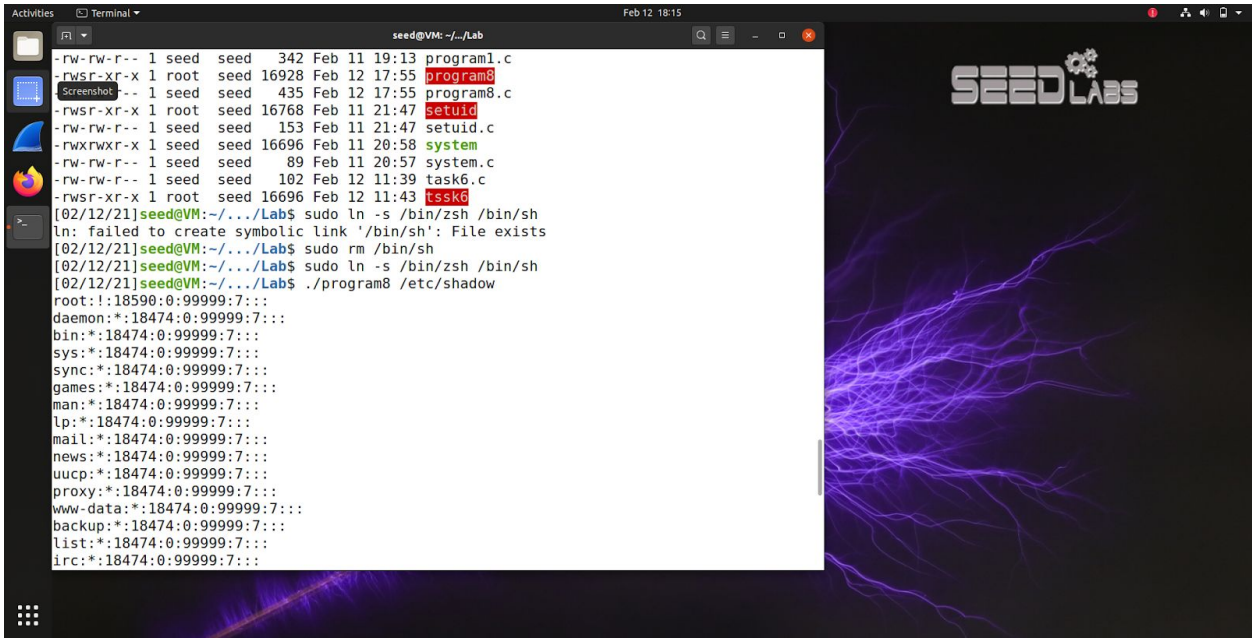
Next, we removed the current link to dash and linked it to insecure zsh.
Now, we were able to run the /etc/shadow file. Hence, Bob could compromise the integrity of the system.

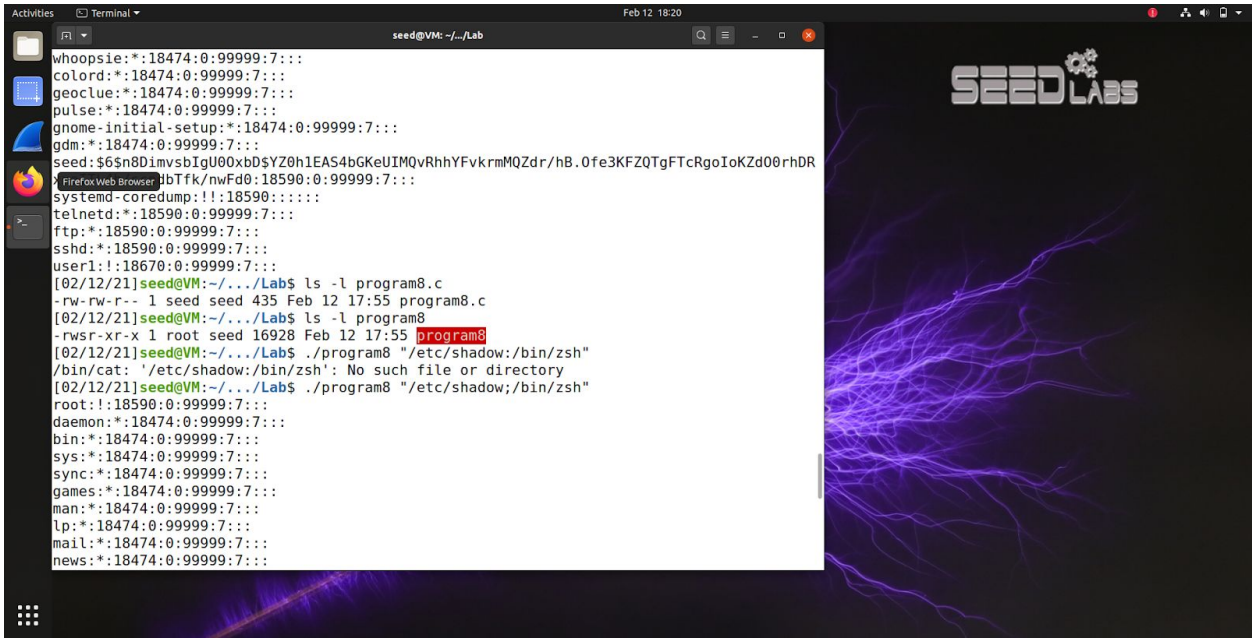
Step 2: Comment out the system(command) statement, and uncomment the execve() statement; the program will use execve() to invoke the command. Compile the program as program8exec, and make it a
root-owned Set-UID.

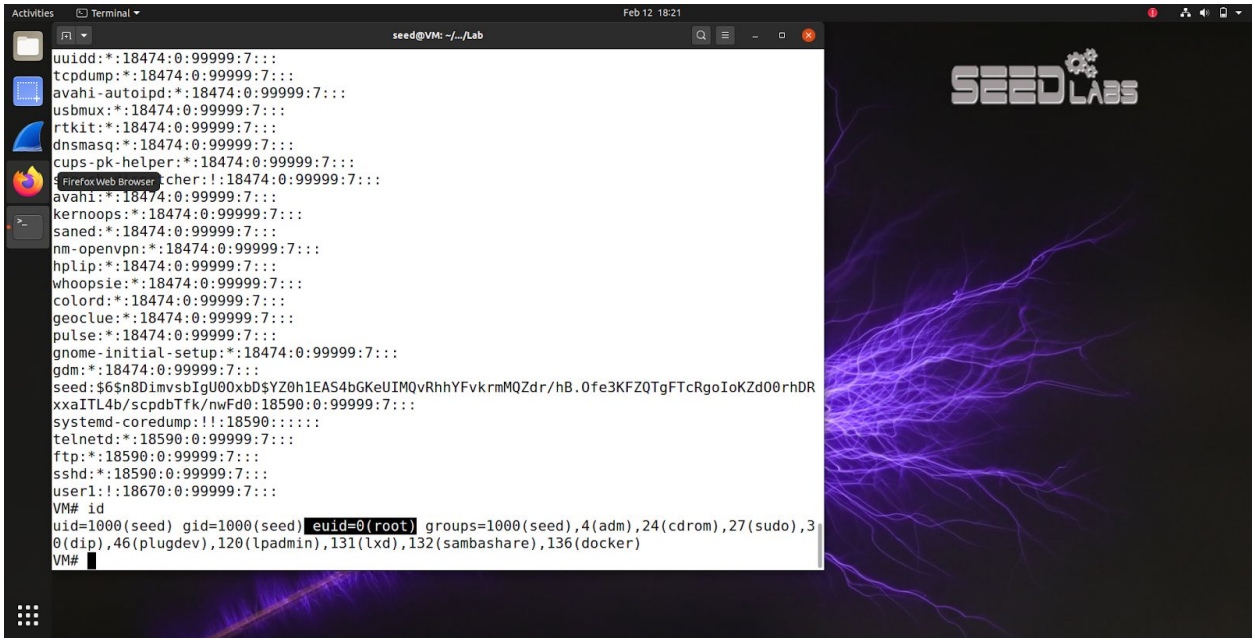
we were not able to run the /etc/shadow file. Because execve() never returns.

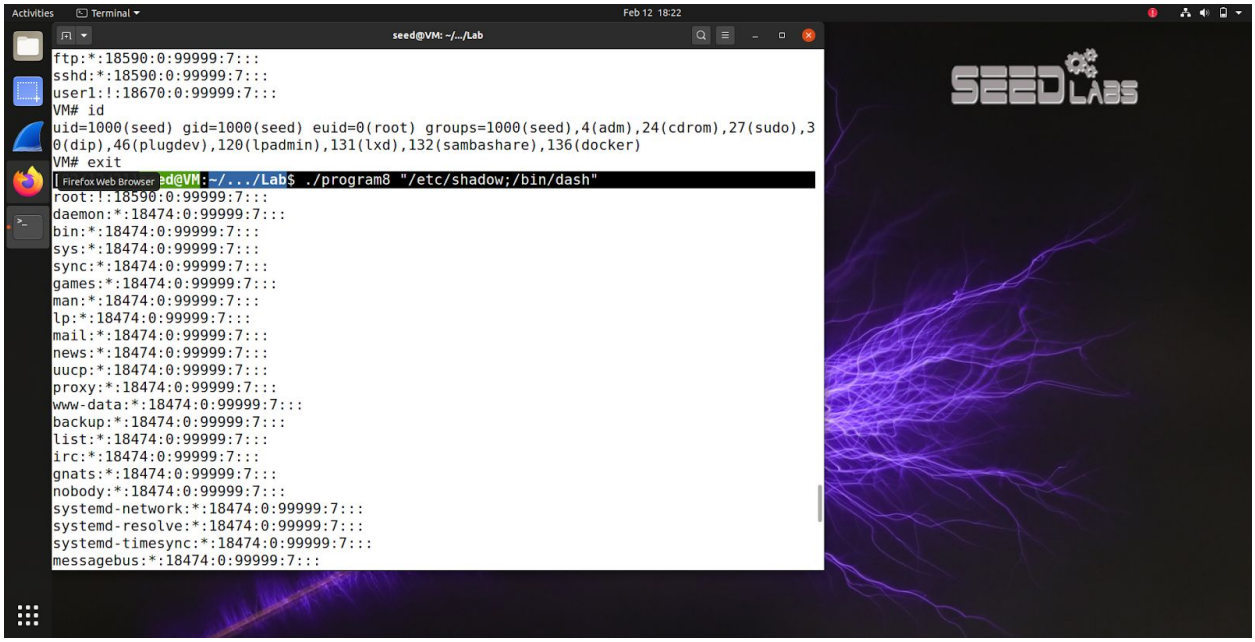


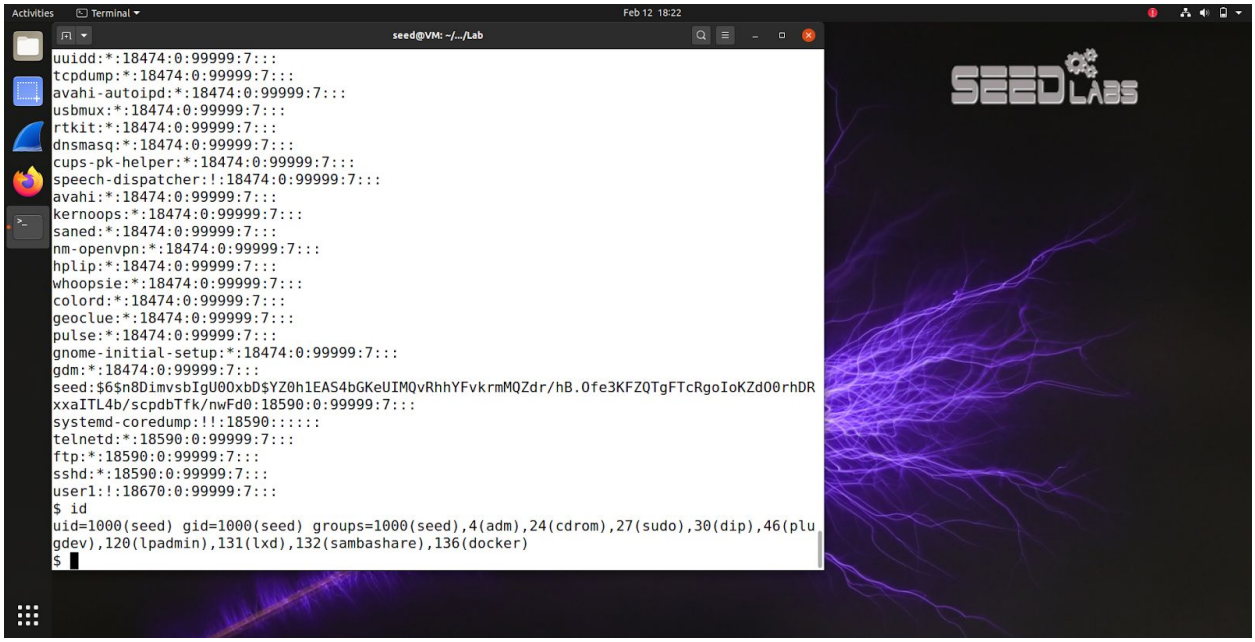

Activities
Terminal
Feb 12 18:11
seed@VM: ~/.../Lab
Files
bash: ./invoke: No such file or directory
[02/12/21]seed@VM:~/.../Lab$ ./program8 /etc/shadow
/bin/cat: /etc/shadow: Permission denied
[02/12/21]seed@VM:~/.../Lab$ ls -l
total 292
-rwxrwxr-x 1 seed seed 16744 Feb 12 11:59 attack
-rw-rw-r-- 1 seed seed 116 Feb 12 11:59 attack.c
-rw-rw-r-- 1 seed seed 3041 Feb 11 19:16 child
-rwxrwxr-x 1 seed seed 16824 Feb 11 20:34 execlprogram
-rwxrwxr-x 1 seed seed 16760 Feb 11 20:29 execprogram
-rw-rw-r-- 1 seed seed 243 Feb 11 20:34 execprogram.c
-rwxrwxr-x 1 seed seed 18688 Feb 12 16:16 libmylib.so.1.0.1
-rw-rw-r-- 1 seed seed 149 Feb 12 16:14 mylib.c
-rw-rw-r-- 1 seed seed 5944 Feb 12 16:15 mylib.o
-rwsr-xr-x 1 root seed 16696 Feb 12 16:34 myprog
-rw-rw-r-- 1 seed seed 71 Feb 12 16:34 myprog.c
-rwsr-xr-x 1 user1 seed 16696 Feb 12 16:55 myprogcopy
-rwxrwxr-x 1 seed seed 16888 Feb 11 18:52 p1child
-rwxrwxr-x 1 seed seed 16888 Feb 11 19:13 p1parent
-rw-rw-r-- 1 seed seed 3042 Feb 11 19:16 parent
-rw-rw-r-- 1 seed seed 342 Feb 11 19:13 program1.c
-rwsr-xr-x 1 root seed 16928 Feb 12 17:55 program8
-rw-rw-r-- 1 seed seed 435 Feb 12 17:55 program8.c
-rwsr-xr-x 1 root seed 16768 Feb 11 21:47 setuid
-rw-rw-r-- 1 seed seed 153 Feb 11 21:47 setuid.c
-rwxrwxr-x 1 seed seed 16696 Feb 11 20:58 system
-rw-rw-r-- 1 seed seed 89 Feb 11 20:57 system.c
-rw-rw-r-- 1 seed seed 102 Feb 12 11:39 task6.c
-rwsr-xr-x 1 root seed 16696 Feb 12 11:43 tssk6
[02/12/21]seed@VM:~/.../Lab$
SEED LABS

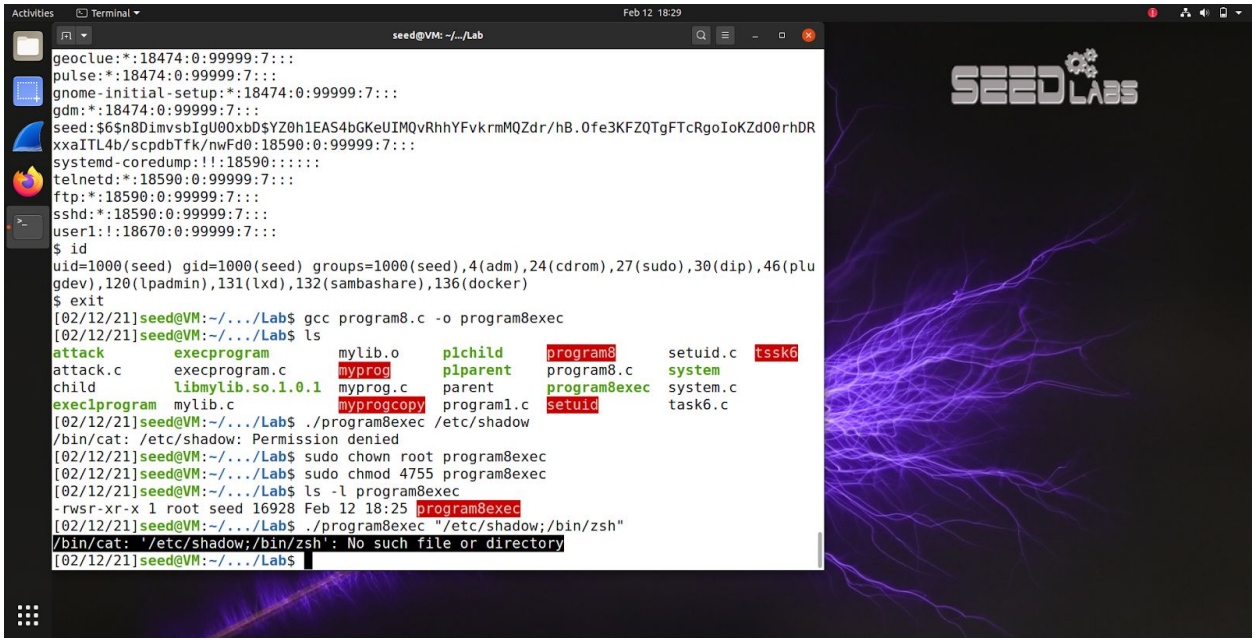

Activities
Terminal
Feb 12 18:15
seed@VM: ~/.../Lab
Screenshot
-rw-rw-r-- 1 seed seed 342 Feb 11 19:13 program1.c
-rwsr-xr-x 1 root seed 16928 Feb 12 17:55 program8
-rw-rw-r-- 1 seed seed 435 Feb 12 17:55 program8.c
-rwsr-xr-x 1 root seed 16768 Feb 11 21:47 setuid
-rw-rw-r-- 1 seed seed 153 Feb 11 21:47 setuid.c
-rwxrwxr-x 1 seed seed 16696 Feb 11 20:58 system
-rw-rw-r-- 1 seed seed 89 Feb 11 20:57 system.c
-rw-rw-r-- 1 seed seed 102 Feb 12 11:39 task6.c
-rwsr-xr-x 1 root seed 16696 Feb 12 11:43 tssk6
[02/12/21]seed@VM:~/.../Lab$ sudo ln -s /bin/zsh /bin/sh
ln: failed to create symbolic link '/bin/sh': File exists
[02/12/21]seed@VM:~/.../Lab$ sudo rm /bin/sh
[02/12/21]seed@VM:~/.../Lab$ sudo ln -s /bin/zsh /bin/sh
[02/12/21]seed@VM:~/.../Lab$ ./program8 /etc/shadow
root:!:18590:0:99999:7:::
daemon:*:18474:0:99999:7:::
bin:*:18474:0:99999:7:::
sys:*:18474:0:99999:7:::
sync:*:18474:0:99999:7:::
games:*:18474:0:99999:7:::
man:*:18474:0:99999:7:::
lp:*:18474:0:99999:7:::
mail:*:18474:0:99999:7:::
news:*:18474:0:99999:7:::
uucp:*:18474:0:99999:7:::
proxy:*:18474:0:99999:7:::
www-data:*:18474:0:99999:7:::
backup:*:18474:0:99999:7:::
list:*:18474:0:99999:7:::
irc:*:18474:0:99999:7:::
SEED LABS


Activities
Terminal
Feb 12 18:20
seed@VM: ~/.../Lab
whoopsie:*:18474:0:99999:7:::
colord:*:18474:0:99999:7:::
geoclue:*:18474:0:99999:7:::
pulse:*:18474:0:99999:7:::
gnome-initial-setup:*:18474:0:99999:7:::
gdm:*:18474:0:99999:7:::
seed:6n8DimvsbIgU0OxbD$YZ0h1EAS4bGKeUIMQvRhhYFvkrmMQZdr/hB.Ofe3KFZQTgFTcRgoIoKZdO0rhDR
xxaITL4b/scpdbTfk/nwFd0:18590:0:99999:7:::
systemd-coredump:!!:18590::::::
telnetd:*:18590:0:99999:7:::
ftp:*:18590:0:99999:7:::
sshd:*:18590:0:99999:7:::
user1:!:18670:0:99999:7:::
[02/12/21]seed@VM:~/.../Lab$ ls -l program8.c
-rw-rw-r-- 1 seed seed 435 Feb 12 17:55 program8.c
[02/12/21]seed@VM:~/.../Lab$ ls -l program8
-rwsr-xr-x 1 root seed 16928 Feb 12 17:55 program8
[02/12/21]seed@VM:~/.../Lab$ ./program8 "/etc/shadow:/bin/zsh"
/bin/cat: '/etc/shadow:/bin/zsh': No such file or directory
[02/12/21]seed@VM:~/.../Lab$ ./program8 "/etc/shadow;/bin/zsh"
root:!:18590:0:99999:7:::
daemon:*:18474:0:99999:7:::
bin:*:18474:0:99999:7:::
sys:*:18474:0:99999:7:::
sync:*:18474:0:99999:7:::
games:*:18474:0:99999:7:::
man:*:18474:0:99999:7:::
lp:*:18474:0:99999:7:::
mail:*:18474:0:99999:7:::
news:*:18474:0:99999:7:::
Firefox Web Browser
SEED LABS


Activities
Terminal
Feb 12 18:21
seed@VM: ~/.../Lab
uuidd:*:18474:0:99999:7:::
tcpdump:*:18474:0:99999:7:::
avahi-autoipd:*:18474:0:99999:7:::
usbmux:*:18474:0:99999:7:::
rtkit:*:18474:0:99999:7:::
dnsmasq:*:18474:0:99999:7:::
cups-pk-helper:*:18474:0:99999:7:::
cher:!:18474:0:99999:7:::
avahi:*:18474:0:99999:7:::
kernoops:*:18474:0:99999:7:::
saned:*:18474:0:99999:7:::
nm-openvpn:*:18474:0:99999:7:::
hplip:*:18474:0:99999:7:::
whoopsie:*:18474:0:99999:7:::
colord:*:18474:0:99999:7:::
geoclue:*:18474:0:99999:7:::
pulse:*:18474:0:99999:7:::
gnome-initial-setup:*:18474:0:99999:7:::
gdm:*:18474:0:99999:7:::
seed:6n8DimvsbIgU0OxbD$YZ0h1EAS4bGKeUIMQvRhhYFvkrmMQZdr/hB.Ofe3KFZQTgFTcRgoIoKZdO0rhDR
xxaITL4b/scpdbTfk/nwFd0:18590:0:99999:7:::
systemd-coredump:!!:18590::::::
telnetd:*:18590:0:99999:7:::
ftp:*:18590:0:99999:7:::
sshd:*:18590:0:99999:7:::
user1:!:18670:0:99999:7:::
VM# id
uid=1000(seed) gid=1000(seed) euid=0(root) groups=1000(seed),4(adm),24(cdrom),27(sudo),3
0(dip),46(plugdev),120(lpadmin),131(lxd),132(sambashare),136(docker)
VM#
Firefox Web Browser
SEED LABS

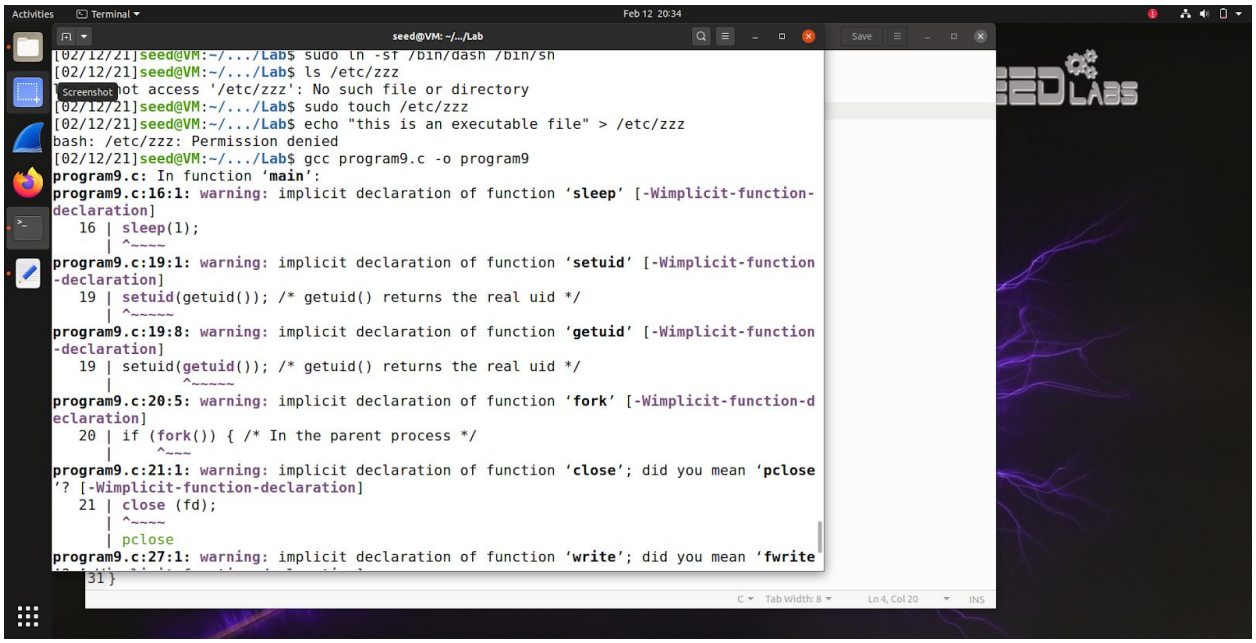

Activities
Terminal
Feb 12 18:22
seed@VM: ~/.../Lab
ftp:*:18590:0:99999:7:::
sshd:*:18590:0:99999:7:::
user1:!:18670:0:99999:7:::
VM# id
uid=1000(seed) gid=1000(seed) euid=0(root) groups=1000(seed),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),120(lpadmin),131(lxd),132(sambashare),136(docker)
VM# exit
Firefox Web Browser
seed@VM:~/.../Lab$ ./program8 "/etc/shadow;/bin/dash"
root:!:18590:0:99999:7:::
daemon:*:18474:0:99999:7:::
bin:*:18474:0:99999:7:::
sys:*:18474:0:99999:7:::
sync:*:18474:0:99999:7:::
games:*:18474:0:99999:7:::
man:*:18474:0:99999:7:::
lp:*:18474:0:99999:7:::
mail:*:18474:0:99999:7:::
news:*:18474:0:99999:7:::
uucp:*:18474:0:99999:7:::
proxy:*:18474:0:99999:7:::
www-data:*:18474:0:99999:7:::
backup:*:18474:0:99999:7:::
list:*:18474:0:99999:7:::
irc:*:18474:0:99999:7:::
gnats:*:18474:0:99999:7:::
nobody:*:18474:0:99999:7:::
systemd-network:*:18474:0:99999:7:::
systemd-resolve:*:18474:0:99999:7:::
systemd-timesync:*:18474:0:99999:7:::
messagebus:*:18474:0:99999:7:::
SEED LABS

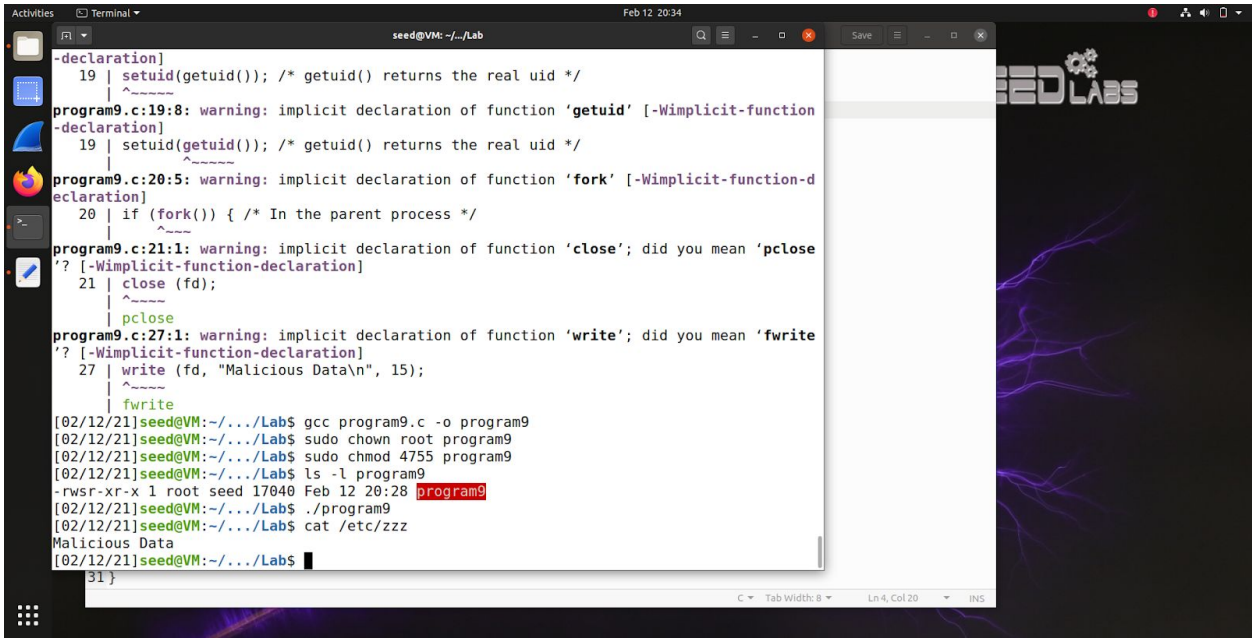

Activities
Terminal
Feb 12 18:22
seed@VM: ~/.../Lab
uuidd:*:18474:0:99999:7:::
tcpdump:*:18474:0:99999:7:::
avahi-autoipd:*:18474:0:99999:7:::
usbmux:*:18474:0:99999:7:::
rtkit:*:18474:0:99999:7:::
dnsmasq:*:18474:0:99999:7:::
cups-pk-helper:*:18474:0:99999:7:::
speech-dispatcher:!:18474:0:99999:7:::
avahi:*:18474:0:99999:7:::
kernoops:*:18474:0:99999:7:::
saned:*:18474:0:99999:7:::
nm-openvpn:*:18474:0:99999:7:::
hplip:*:18474:0:99999:7:::
whoopsie:*:18474:0:99999:7:::
colord:*:18474:0:99999:7:::
geoclue:*:18474:0:99999:7:::
pulse:*:18474:0:99999:7:::
gnome-initial-setup:*:18474:0:99999:7:::
gdm:*:18474:0:99999:7:::
seed:6n8DimvsbIgU0OxbD$YZ0h1EAS4bGKeUIMQvRhhYFvkrmMQZdr/hB.Ofe3KFZQTgFTcRgoIoKZdO0rhDRxxaITL4b/scpdbTfk/nwFd0:18590:0:99999:7:::
systemd-coredump:!!:18590::::::
telnetd:*:18590:0:99999:7:::
ftp:*:18590:0:99999:7:::
sshd:*:18590:0:99999:7:::
user1:!:18670:0:99999:7:::
$ id
uid=1000(seed) gid=1000(seed) groups=1000(seed),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),120(lpadmin),131(lxd),132(sambashare),136(docker)
$
SEED LABS



Task 9: Capability Leaking

As we can see, the file has been modifid, the reason is file `zzz` is opened before set uid. To avoid this problem we can move `setuid(getuid())` to the front of `open()` function.




Activities
Terminal
Feb 12 20:34
seed@VM: ~/.../Lab
Save
-declaration]
19 | setuid(getuid()); /* getuid() returns the real uid */
| ^~~~~~
program9.c:19:8: warning: implicit declaration of function ‘getuid’ [-Wimplicit-function-declaration]
19 | setuid(getuid()); /* getuid() returns the real uid */
| ^~~~~~
program9.c:20:5: warning: implicit declaration of function ‘fork’ [-Wimplicit-function-declaration]
20 | if (fork()) { /* In the parent process */
| ^~~~
program9.c:21:1: warning: implicit declaration of function ‘close’; did you mean ‘pclose’? [-Wimplicit-function-declaration]
21 | close (fd);
| ^~~~~
| pclose
program9.c:27:1: warning: implicit declaration of function ‘write’; did you mean ‘fwrite’? [-Wimplicit-function-declaration]
27 | write (fd, "Malicious Data\n", 15);
| ^~~~~
| fwrite
[02/12/21]seed@VM:~/.../Lab$ gcc program9.c -o program9
[02/12/21]seed@VM:~/.../Lab$ sudo chown root program9
[02/12/21]seed@VM:~/.../Lab$ sudo chmod 4755 program9
[02/12/21]seed@VM:~/.../Lab$ ls -l program9
-rwsr-xr-x 1 root seed 17040 Feb 12 20:28 program9
[02/12/21]seed@VM:~/.../Lab$ ./program9
[02/12/21]seed@VM:~/.../Lab$ cat /etc/zzz
Malicious Data
[02/12/21]seed@VM:~/.../Lab$
31 }
C
Tab Width: 8
Ln 4, Col 20
INS