Carlos Reyes

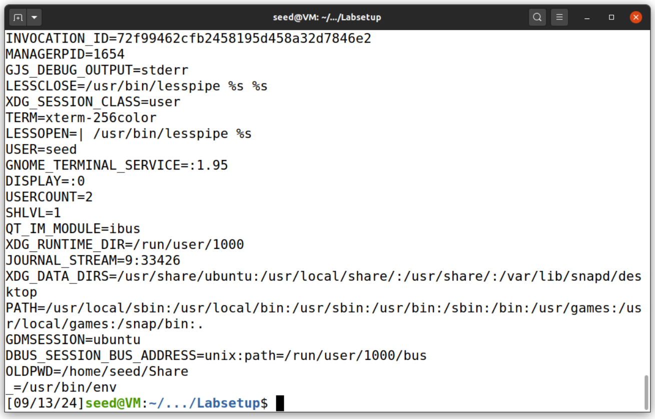
9/24/2024

CS 574

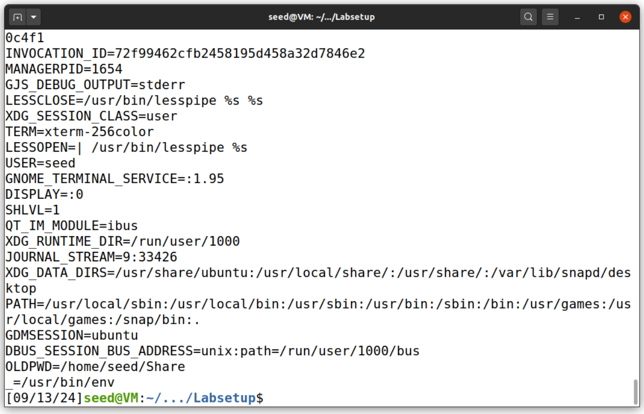
Security Assignment 1

Task 1:

We observe that we can set and unset environment variables. We can also view the current shells environment variables by printenv and also we can filter through them by piping and using the grep command in order to filter out or find certain variables with certain keywords.



```
INVOCATION_ID=72f99462cfb2458195d458a32d7846e2
MANAGERPID=1654
GJS_DEBUG_OUTPUT=stderr
LESSCLOSE=/usr/bin/lesspipe %s %s
XDG_SESSION_CLASS=user
TERM=xterm-256color
LESSOPEN=| /usr/bin/lesspipe %s
USER=seed
GNOME_TERMINAL_SERVICE=:1.95
DISPLAY=:0
USERCOUNT=2
SHLVL=1
QT_IM_MODULE=ibus
XDG_RUNTIME_DIR=/run/user/1000
JOURNAL_STREAM=9:33426
XDG_DATA_DIRS=/usr/share/ubuntu:/usr/local/share/:/usr/share/:/var/lib/snapd/des
ktop
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/us
r/local/games:/snap/bin:.
GDMSESSION=ubuntu
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
OLDPWD=/home/seed/Share
_=/usr/bin/env
[09/13/24]seed@VM:~/.../Labsetup$ 
```

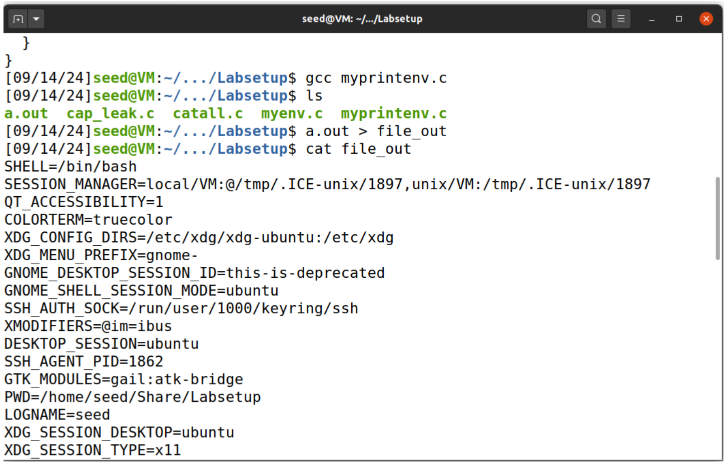


```
0c4f1
INVOCATION_ID=72f99462cfb2458195d458a32d7846e2
MANAGERPID=1654
GJS_DEBUG_OUTPUT=stderr
LESSCLOSE=/usr/bin/lesspipe %s %s
XDG_SESSION_CLASS=user
TERM=xterm-256color
LESSOPEN=| /usr/bin/lesspipe %s
USER=seed
GNOME_TERMINAL_SERVICE=:1.95
DISPLAY=:0
SHLVL=1
QT_IM_MODULE=ibus
XDG_RUNTIME_DIR=/run/user/1000
JOURNAL_STREAM=9:33426
XDG_DATA_DIRS=/usr/share/ubuntu:/usr/local/share/:/usr/share/:/var/lib/snapd/des
ktop
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/us
r/local/games:/snap/bin:.
GDMSESSION=ubuntu
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
OLDPWD=/home/seed/Share
_=/usr/bin/env
[09/13/24]seed@VM:~/.../Labsetup$
```

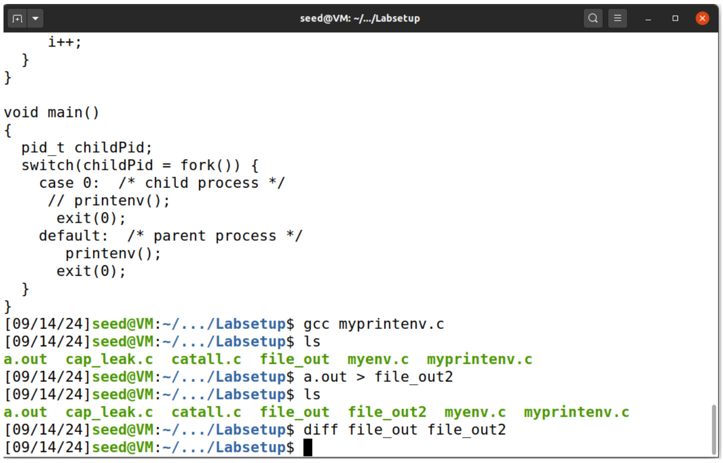
Task 2:

In this first part we are running our programs which sets up the double pointer to get the external variable array from the current shell called environ. In this part we are creating a child process then proceeding to print out our environment variables to our standard output and exiting with code zero. We are directing our output to our file in this case use > which directs the environment variables to that file.

In this second part we have created another child process and the same process from above takes place. We can see that by using the diff command there and no differences in the environment variables so it means that the same environment variables are inherited from the parent process.



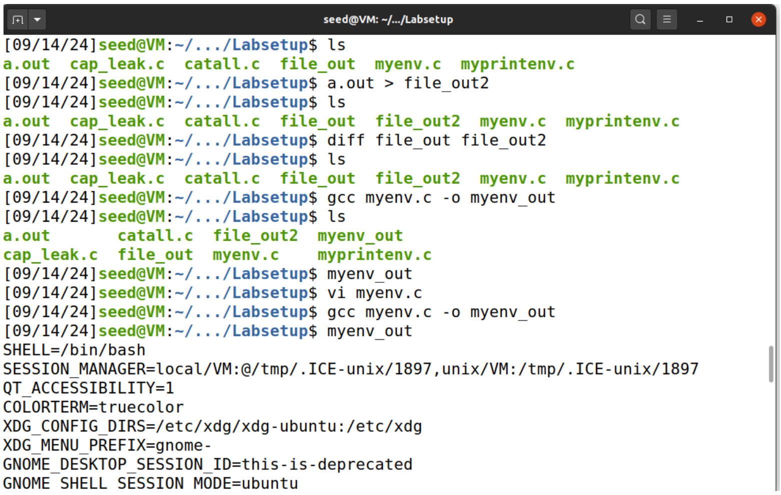
```
  }
}
[09/14/24]seed@VM:~/.../Labsetup$ gcc myprintenv.c
[09/14/24]seed@VM:~/.../Labsetup$ ls
a.out  cap_leak.c  catall.c  myenv.c  myprintenv.c
[09/14/24]seed@VM:~/.../Labsetup$ a.out > file_out
[09/14/24]seed@VM:~/.../Labsetup$ cat file_out
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/1897,unix/VM:/tmp/.ICE-unix/1897
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=1862
GTK_MODULES=gail:atk-bridge
PWD=/home/seed/Share/Labsetup
LOGNAME=seed
XDG_SESSION_DESKTOP=ubuntu
XDG_SESSION_TYPE=x11
```



```
     i++;
  }
}

void main()
{
  pid_t childPid;
  switch(childPid = fork()) {
    case 0:  /* child process */
     // printenv();
      exit(0);
    default:  /* parent process */
       printenv();
      exit(0);
  }
}
[09/14/24]seed@VM:~/.../Labsetup$ gcc myprintenv.c
[09/14/24]seed@VM:~/.../Labsetup$ ls
a.out  cap_leak.c  catall.c  file_out  myenv.c  myprintenv.c
[09/14/24]seed@VM:~/.../Labsetup$ a.out > file_out2
[09/14/24]seed@VM:~/.../Labsetup$ ls
a.out  cap_leak.c  catall.c  file_out  file_out2  myenv.c  myprintenv.c
[09/14/24]seed@VM:~/.../Labsetup$ diff file_out file_out2
[09/14/24]seed@VM:~/.../Labsetup$ 
```

Task 3:

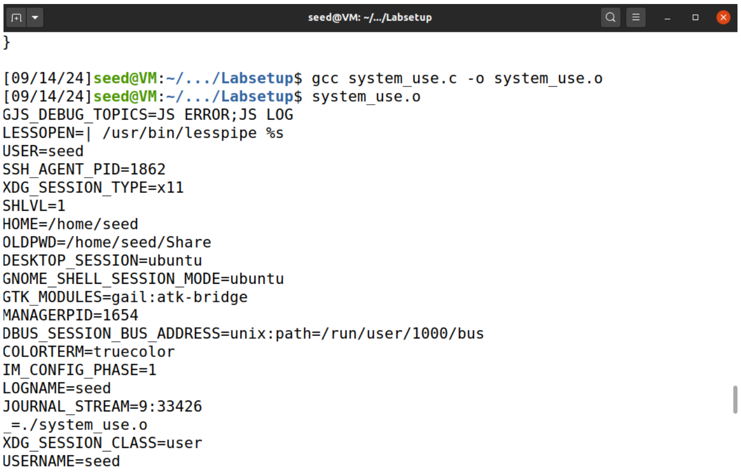
Since our execsve function is not creating a child process our environment variables are not inherited. We are running a new program inside the calling process and our text data and bss are overwritten by the program loaded so we have no environment variables available in this case. In the second case we are passing environ which is our environment variable double pointer with all of our environment variables therefore the environment variables are available in this case by passing them as a variable data. That's the safest way to do it but we do have to take extra steps in order to make our environment variables available.



```
[09/14/24]seed@VM:~/.../Labsetup$ ls
a.out  cap_leak.c  catall.c  file_out  myenv.c  myprintenv.c
[09/14/24]seed@VM:~/.../Labsetup$ a.out > file_out2
[09/14/24]seed@VM:~/.../Labsetup$ ls
a.out  cap_leak.c  catall.c  file_out  file_out2  myenv.c  myprintenv.c
[09/14/24]seed@VM:~/.../Labsetup$ diff file_out file_out2
[09/14/24]seed@VM:~/.../Labsetup$ ls
a.out  cap_leak.c  catall.c  file_out  file_out2  myenv.c  myprintenv.c
[09/14/24]seed@VM:~/.../Labsetup$ gcc myenv.c -o myenv_out
[09/14/24]seed@VM:~/.../Labsetup$ ls
a.out       catall.c  file_out2  myenv_out
cap_leak.c  file_out  myenv.c    myprintenv.c
[09/14/24]seed@VM:~/.../Labsetup$ myenv_out
[09/14/24]seed@VM:~/.../Labsetup$ vi myenv.c
[09/14/24]seed@VM:~/.../Labsetup$ gcc myenv.c -o myenv_out
[09/14/24]seed@VM:~/.../Labsetup$ myenv_out
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/1897,unix/VM:/tmp/.ICE-unix/1897
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 4:

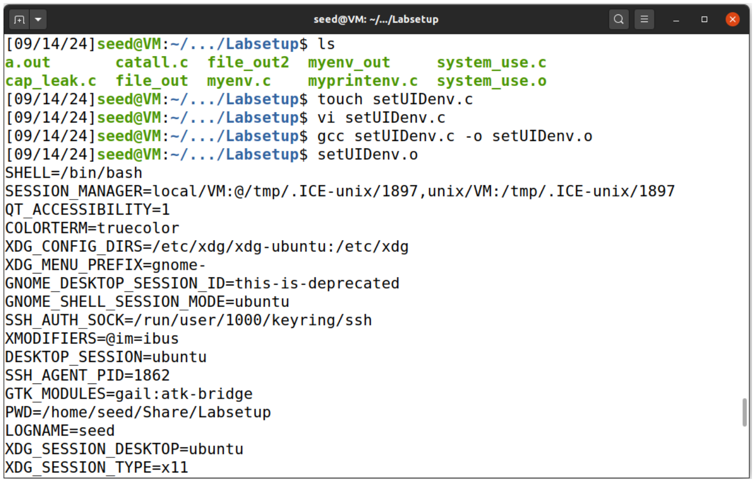
In this task we can see that our environment variables are inherited by the child process.



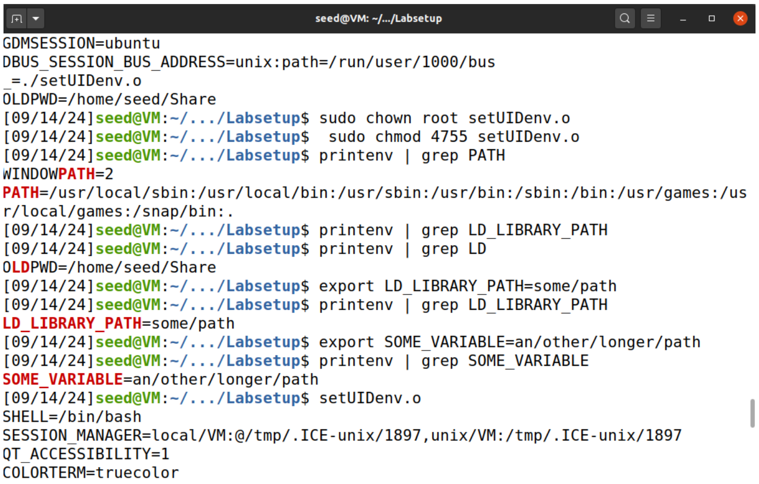
```
}

[09/14/24]seed@VM:~/.../Labsetup$ gcc system_use.c -o system_use.o
[09/14/24]seed@VM:~/.../Labsetup$ system_use.o
GJS_DEBUG_TOPICS=JS ERROR;JS LOG
LESSOPEN=| /usr/bin/lesspipe %s
USER=seed
SSH_AGENT_PID=1862
XDG_SESSION_TYPE=x11
SHLVL=1
HOME=/home/seed
OLDPWD=/home/seed/Share
DESKTOP_SESSION=ubuntu
GNOME_SHELL_SESSION_MODE=ubuntu
GTK_MODULES=gail:atk-bridge
MANAGERPID=1654
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
COLORTERM=truecolor
IM_CONFIG_PHASE=1
LOGNAME=seed
JOURNAL_STREAM=9:33426
_=./system_use.o
XDG_SESSION_CLASS=user
USERNAME=seed
```

Task 5:

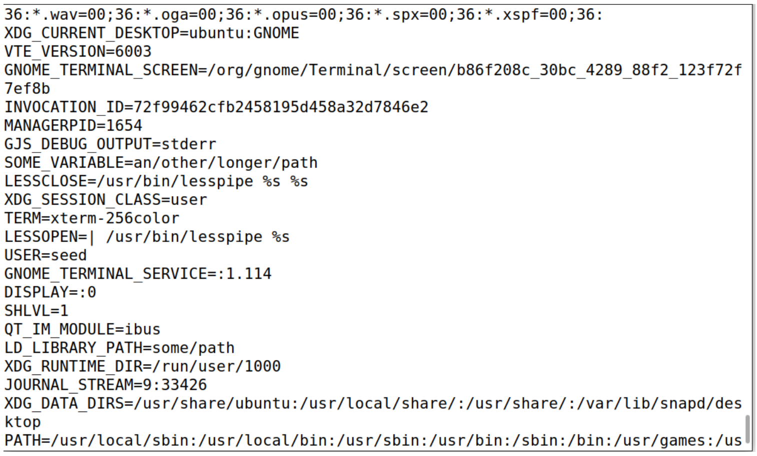
In this case since we set our variable in the shell process and our shell process in the parent of the process started by the setuid program our environment variables are inherited.



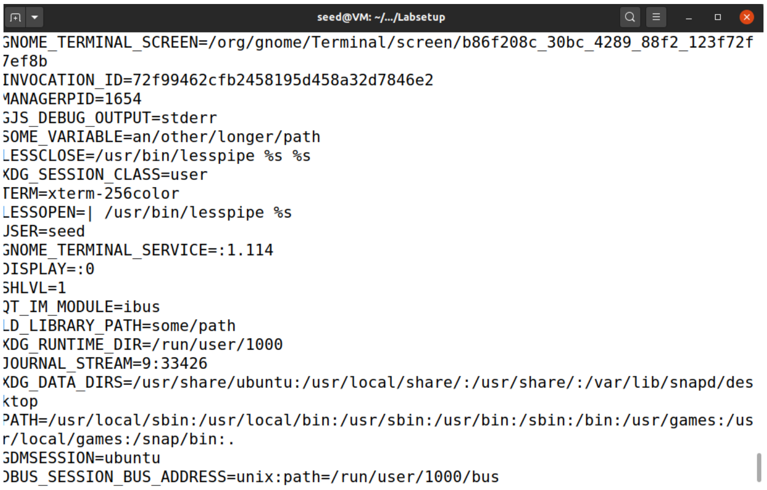
```
[09/14/24]seed@VM:~/.../Labsetup$ ls
a.out       catall.c  file_out2  myenv_out     system_use.c
cap_leak.c  file_out  myenv.c    myprintenv.c  system_use.o
[09/14/24]seed@VM:~/.../Labsetup$ touch setUIDenv.c
[09/14/24]seed@VM:~/.../Labsetup$ vi setUIDenv.c
[09/14/24]seed@VM:~/.../Labsetup$ gcc setUIDenv.c -o setUIDenv.o
[09/14/24]seed@VM:~/.../Labsetup$ setUIDenv.o
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/1897,unix/VM:/tmp/.ICE-unix/1897
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=1862
GTK_MODULES=gail:atk-bridge
PWD=/home/seed/Share/Labsetup
LOGNAME=seed
XDG_SESSION_DESKTOP=ubuntu
XDG_SESSION_TYPE=x11
```



```
GDMSESSION=ubuntu
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
_=./setUIDenv.o
OLDPWD=/home/seed/Share
[09/14/24]seed@VM:~/.../Labsetup$ sudo chown root setUIDenv.o
[09/14/24]seed@VM:~/.../Labsetup$  sudo chmod 4755 setUIDenv.o
[09/14/24]seed@VM:~/.../Labsetup$ printenv | grep PATH
WINDOWPATH=2
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/us
r/local/games:/snap/bin:.
[09/14/24]seed@VM:~/.../Labsetup$ printenv | grep LD_LIBRARY_PATH
[09/14/24]seed@VM:~/.../Labsetup$ printenv | grep LD
OLDPWD=/home/seed/Share
[09/14/24]seed@VM:~/.../Labsetup$ export LD_LIBRARY_PATH=some/path
[09/14/24]seed@VM:~/.../Labsetup$ printenv | grep LD_LIBRARY_PATH
LD_LIBRARY_PATH=some/path
[09/14/24]seed@VM:~/.../Labsetup$ export SOME_VARIABLE=an/other/longer/path
[09/14/24]seed@VM:~/.../Labsetup$ printenv | grep SOME_VARIABLE
SOME_VARIABLE=an/other/longer/path
[09/14/24]seed@VM:~/.../Labsetup$ setUIDenv.o
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/1897,unix/VM:/tmp/.ICE-unix/1897
QT_ACCESSIBILITY=1
COLORTERM=truecolor
```



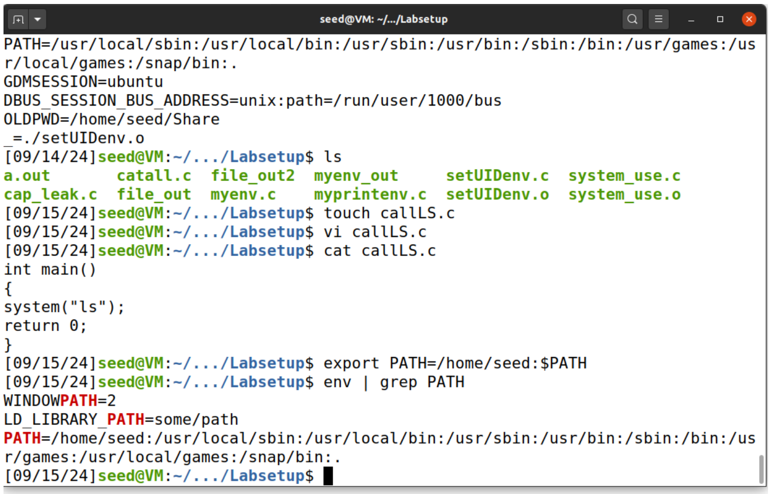
```
36:*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:
XDG_CURRENT_DESKTOP=ubuntu:GNOME
VTE_VERSION=6003
GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/b86f208c_30bc_4289_88f2_123f72f
7ef8b
INVOCATION_ID=72f99462cfb2458195d458a32d7846e2
MANAGERPID=1654
GJS_DEBUG_OUTPUT=stderr
SOME_VARIABLE=an/other/longer/path
LESSCLOSE=/usr/bin/lesspipe %s %s
XDG_SESSION_CLASS=user
TERM=xterm-256color
LESSOPEN=| /usr/bin/lesspipe %s
USER=seed
GNOME_TERMINAL_SERVICE=:1.114
DISPLAY=:0
SHLVL=1
QT_IM_MODULE=ibus
LD_LIBRARY_PATH=some/path
XDG_RUNTIME_DIR=/run/user/1000
JOURNAL_STREAM=9:33426
XDG_DATA_DIRS=/usr/share/ubuntu:/usr/local/share/:/usr/share/:/var/lib/snapd/des
ktop
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/us
```



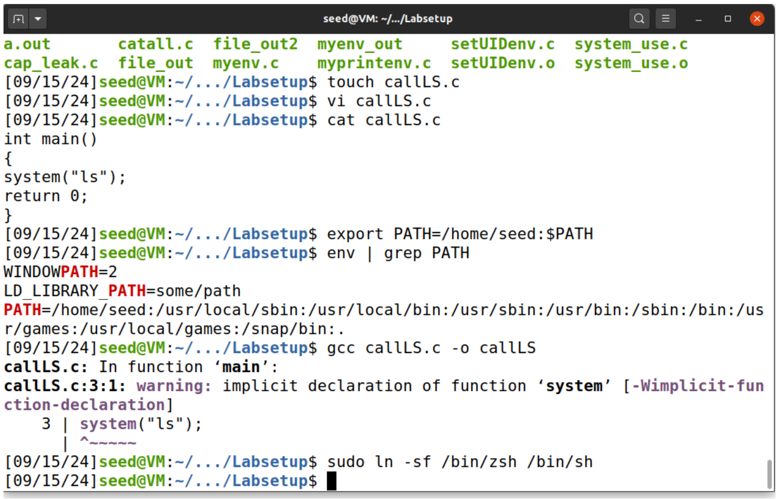
```
GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/b86f208c_30bc_4289_88f2_123f72f
7ef8b
INVOCATION_ID=72f99462cfb2458195d458a32d7846e2
MANAGERPID=1654
GJS_DEBUG_OUTPUT=stderr
SOME_VARIABLE=an/other/longer/path
LESSCLOSE=/usr/bin/lesspipe %s %s
XDG_SESSION_CLASS=user
TERM=xterm-256color
LESSOPEN=| /usr/bin/lesspipe %s
USER=seed
GNOME_TERMINAL_SERVICE=:1.114
DISPLAY=:0
SHLVL=1
QT_IM_MODULE=ibus
LD_LIBRARY_PATH=some/path
XDG_RUNTIME_DIR=/run/user/1000
JOURNAL_STREAM=9:33426
XDG_DATA_DIRS=/usr/share/ubuntu:/usr/local/share/:/usr/share/:/var/lib/snapd/des
ktop
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/us
r/local/games:/snap/bin:.
GDMSESSION=ubuntu
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
```

Task 6:

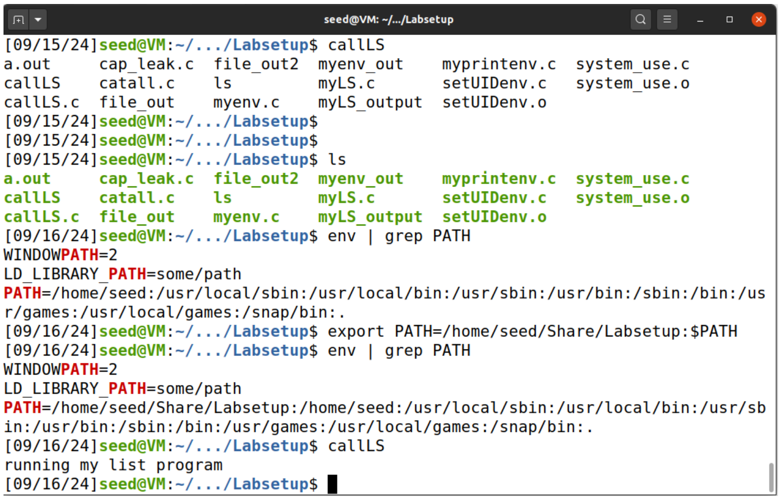
By changing our path variable, we can direct our shell to look inside that directory first for the command. We can make our own ls command and run it. Using a system as a set uid program is dangerous since we have a EUID for the owner of the program which is root in this case so the running system will look for our program in that directory we specified first and run our list program instead of the right one. In doing so we run our own list programs with root privilege since its a set uid program with the owner of root.



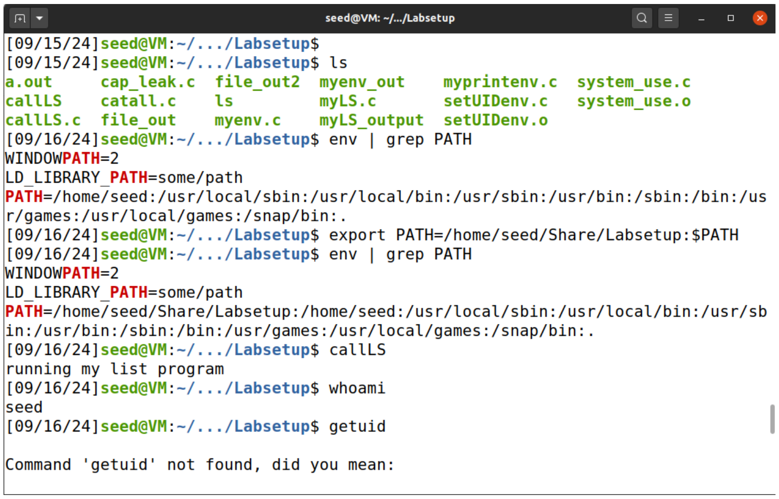
```
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/us
r/local/games:/snap/bin:.
GDMSESSION=ubuntu
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
OLDPWD=/home/seed/Share
_=./setUIDenv.o
[09/14/24]seed@VM:~/.../Labsetup$ ls
a.out       catall.c  file_out2  myenv_out     setUIDenv.c  system_use.c
cap_leak.c  file_out  myenv.c    myprintenv.c  setUIDenv.o  system_use.o
[09/15/24]seed@VM:~/.../Labsetup$ touch callLS.c
[09/15/24]seed@VM:~/.../Labsetup$ vi callLS.c
[09/15/24]seed@VM:~/.../Labsetup$ cat callLS.c
int main()
{
system("ls");
return 0;
}
[09/15/24]seed@VM:~/.../Labsetup$ export PATH=/home/seed:$PATH
[09/15/24]seed@VM:~/.../Labsetup$ env | grep PATH
WINDOWPATH=2
LD_LIBRARY_PATH=some/path
PATH=/home/seed:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/us
r/games:/usr/local/games:/snap/bin:.
[09/15/24]seed@VM:~/.../Labsetup$ 
```



```
a.out       catall.c  file_out2  myenv_out     setUIDenv.c  system_use.c
cap_leak.c  file_out  myenv.c    myprintenv.c  setUIDenv.o  system_use.o
[09/15/24]seed@VM:~/.../Labsetup$ touch callLS.c
[09/15/24]seed@VM:~/.../Labsetup$ vi callLS.c
[09/15/24]seed@VM:~/.../Labsetup$ cat callLS.c
int main()
{
system("ls");
return 0;
}
[09/15/24]seed@VM:~/.../Labsetup$ export PATH=/home/seed:$PATH
[09/15/24]seed@VM:~/.../Labsetup$ env | grep PATH
WINDOWPATH=2
LD_LIBRARY_PATH=some/path
PATH=/home/seed:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/us
r/games:/usr/local/games:/snap/bin:.
[09/15/24]seed@VM:~/.../Labsetup$ gcc callLS.c -o callLS
callLS.c: In function ‘main’:
callLS.c:3:1: warning: implicit declaration of function ‘system’ [-Wimplicit-fun
ction-declaration]
    3 | system("ls");
      | ^~~~~~
[09/15/24]seed@VM:~/.../Labsetup$ sudo ln -sf /bin/zsh /bin/sh
[09/15/24]seed@VM:~/.../Labsetup$ 
```



```
[09/15/24]seed@VM:~/.../Labsetup$ callLS
a.out     cap_leak.c  file_out2  myenv_out     myprintenv.c  system_use.c
callLS    catall.c    ls         myLS.c        setUIDenv.c   system_use.o
callLS.c  file_out    myenv.c    myLS_output   setUIDenv.o
[09/15/24]seed@VM:~/.../Labsetup$
[09/15/24]seed@VM:~/.../Labsetup$
[09/15/24]seed@VM:~/.../Labsetup$ ls
a.out     cap_leak.c  file_out2  myenv_out     myprintenv.c  system_use.c
callLS    catall.c    ls         myLS.c        setUIDenv.c   system_use.o
callLS.c  file_out    myenv.c    myLS_output   setUIDenv.o
[09/16/24]seed@VM:~/.../Labsetup$ env | grep PATH
WINDOWPATH=2
LD_LIBRARY_PATH=some/path
PATH=/home/seed:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/us
r/games:/usr/local/games:/snap/bin:.
[09/16/24]seed@VM:~/.../Labsetup$ export PATH=/home/seed/Share/Labsetup:$PATH
[09/16/24]seed@VM:~/.../Labsetup$ env | grep PATH
WINDOWPATH=2
LD_LIBRARY_PATH=some/path
PATH=/home/seed/Share/Labsetup:/home/seed:/usr/local/sbin:/usr/local/bin:/usr/sb
in:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin:.
[09/16/24]seed@VM:~/.../Labsetup$ callLS
running my list program
[09/16/24]seed@VM:~/.../Labsetup$ 
```



```
[09/15/24]seed@VM:~/.../Labsetup$
[09/15/24]seed@VM:~/.../Labsetup$ ls
a.out     cap_leak.c  file_out2  myenv_out     myprintenv.c  system_use.c
callLS    catall.c    ls         myLS.c        setUIDenv.c   system_use.o
callLS.c  file_out    myenv.c    myLS_output   setUIDenv.o
[09/16/24]seed@VM:~/.../Labsetup$ env | grep PATH
WINDOWPATH=2
LD_LIBRARY_PATH=some/path
PATH=/home/seed:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/us
r/games:/usr/local/games:/snap/bin:.
[09/16/24]seed@VM:~/.../Labsetup$ export PATH=/home/seed/Share/Labsetup:$PATH
[09/16/24]seed@VM:~/.../Labsetup$ env | grep PATH
WINDOWPATH=2
LD_LIBRARY_PATH=some/path
PATH=/home/seed/Share/Labsetup:/home/seed:/usr/local/sbin:/usr/local/bin:/usr/sb
in:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin:.
[09/16/24]seed@VM:~/.../Labsetup$ callLS
running my list program
[09/16/24]seed@VM:~/.../Labsetup$ whoami
seed
[09/16/24]seed@VM:~/.../Labsetup$ getuid

Command 'getuid' not found, did you mean:
```

Task 7:

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

In this case our program runs our malicious library program since when running our program it looks in the directory we set up on ldpreload and finds our library file.

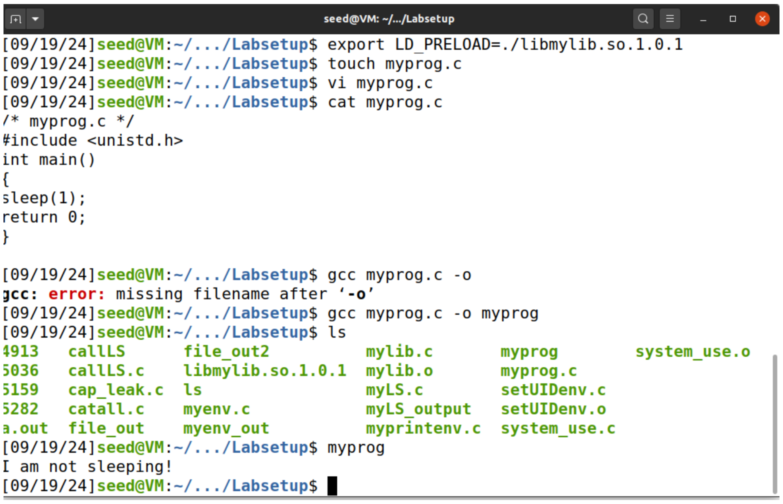
Make myprog a Set-UID root program, and run it as a normal user:

In this case we have set up a set uid program and even though we exported our variable with the path to look for our own library our set uid program has a mechanism that does not copy these two environment variables to the child process so in this case the set uid program runds the original library.

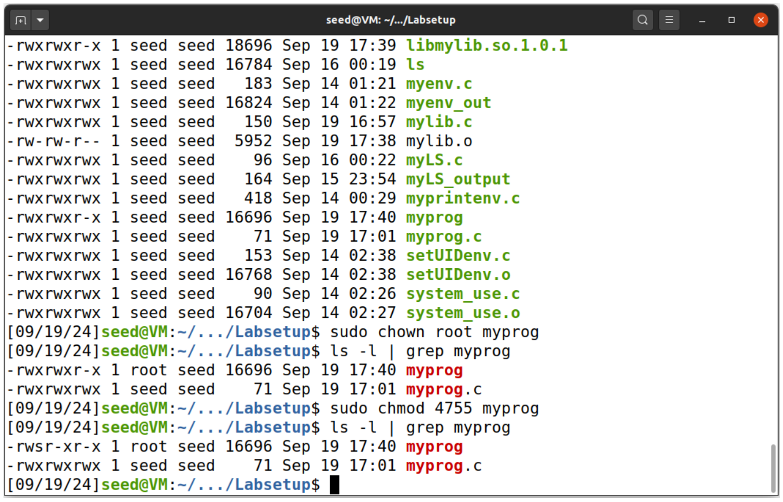
Make myprog a Set-UID root program, export the LD PRELOAD environment variable again in the root account and run it:

In this case even tho we have exported our variable using our root account our program is still a set uid program so the same mechanism applies and the two environment variables are not copied tot he child process started by the set uid.

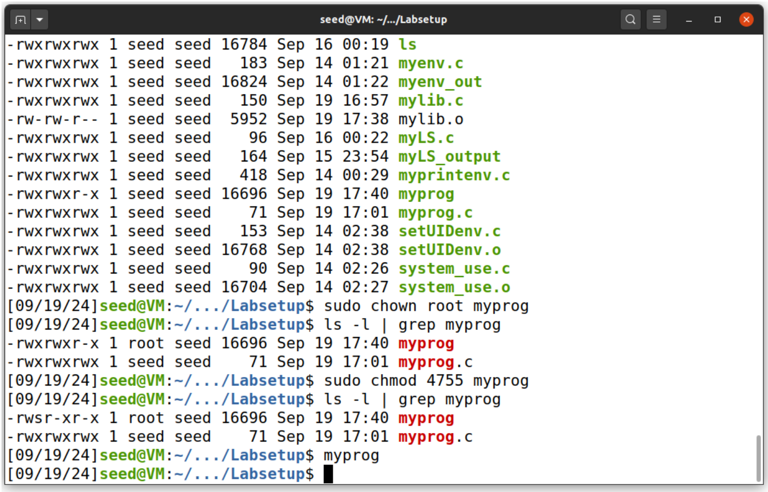
Even tho we made it a set uid program and exported the variable it has the same effect since the variable isn't copies since its still a set uid program regardless of the owner



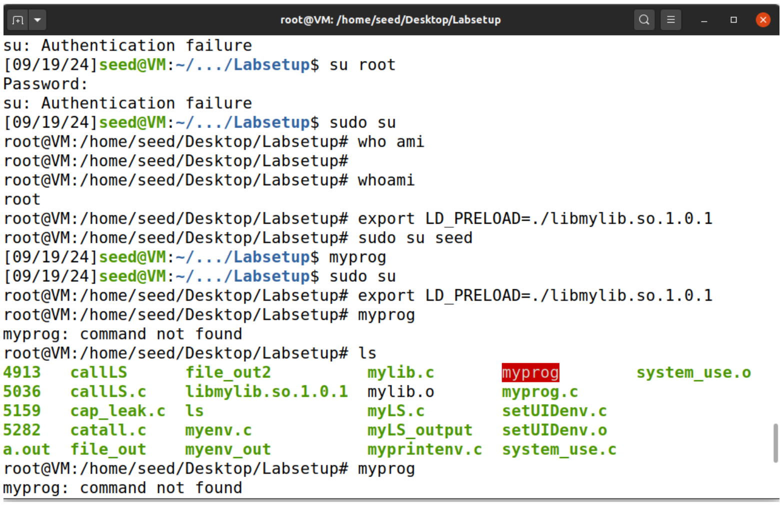
```
[09/19/24]seed@VM:~/.../Labsetup$ export LD_PRELOAD=./libmylib.so.1.0.1
[09/19/24]seed@VM:~/.../Labsetup$ touch myprog.c
[09/19/24]seed@VM:~/.../Labsetup$ vi myprog.c
[09/19/24]seed@VM:~/.../Labsetup$ cat myprog.c
/* myprog.c */
#include <unistd.h>
int main()
{
sleep(1);
return 0;
}

[09/19/24]seed@VM:~/.../Labsetup$ gcc myprog.c -o
gcc: error: missing filename after ‘-o’
[09/19/24]seed@VM:~/.../Labsetup$ gcc myprog.c -o myprog
[09/19/24]seed@VM:~/.../Labsetup$ ls
4913   callLS      file_out2          mylib.c       myprog        system_use.o
5036   callLS.c    libmylib.so.1.0.1  mylib.o       myprog.c
5159   cap_leak.c  ls                 myLS.c        setUIDenv.c
5282   catall.c    myenv.c            myLS_output   setUIDenv.o
a.out  file_out    myenv_out          myprintenv.c  system_use.c
[09/19/24]seed@VM:~/.../Labsetup$ myprog
I am not sleeping!
[09/19/24]seed@VM:~/.../Labsetup$ 
```



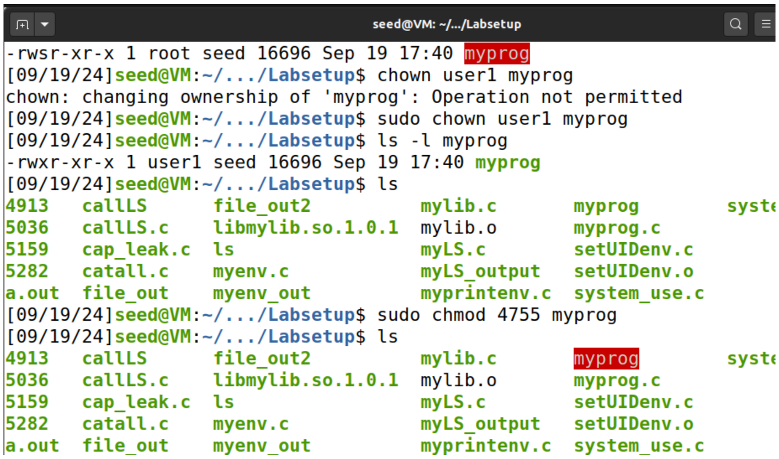
```
-rwxrwxr-x 1 seed seed 18696 Sep 19 17:39 libmylib.so.1.0.1
-rwxrwxrwx 1 seed seed 16784 Sep 16 00:19 ls
-rwxrwxrwx 1 seed seed   183 Sep 14 01:21 myenv.c
-rwxrwxrwx 1 seed seed 16824 Sep 14 01:22 myenv_out
-rwxrwxrwx 1 seed seed   150 Sep 19 16:57 mylib.c
-rw-rw-r-- 1 seed seed  5952 Sep 19 17:38 mylib.o
-rwxrwxrwx 1 seed seed    96 Sep 16 00:22 myLS.c
-rwxrwxrwx 1 seed seed   164 Sep 15 23:54 myLS_output
-rwxrwxrwx 1 seed seed   418 Sep 14 00:29 myprintenv.c
-rwxrwxr-x 1 seed seed 16696 Sep 19 17:40 myprog
-rwxrwxrwx 1 seed seed    71 Sep 19 17:01 myprog.c
-rwxrwxrwx 1 seed seed   153 Sep 14 02:38 setUIDenv.c
-rwxrwxrwx 1 seed seed 16768 Sep 14 02:38 setUIDenv.o
-rwxrwxrwx 1 seed seed    90 Sep 14 02:26 system_use.c
-rwxrwxrwx 1 seed seed 16704 Sep 14 02:27 system_use.o
[09/19/24]seed@VM:~/.../Labsetup$ sudo chown root myprog
[09/19/24]seed@VM:~/.../Labsetup$ ls -l | grep myprog
-rwxrwxr-x 1 root seed 16696 Sep 19 17:40 myprog
-rwxrwxrwx 1 seed seed    71 Sep 19 17:01 myprog.c
[09/19/24]seed@VM:~/.../Labsetup$ sudo chmod 4755 myprog
[09/19/24]seed@VM:~/.../Labsetup$ ls -l | grep myprog
-rwsr-xr-x 1 root seed 16696 Sep 19 17:40 myprog
-rwxrwxrwx 1 seed seed    71 Sep 19 17:01 myprog.c
[09/19/24]seed@VM:~/.../Labsetup$ 
```



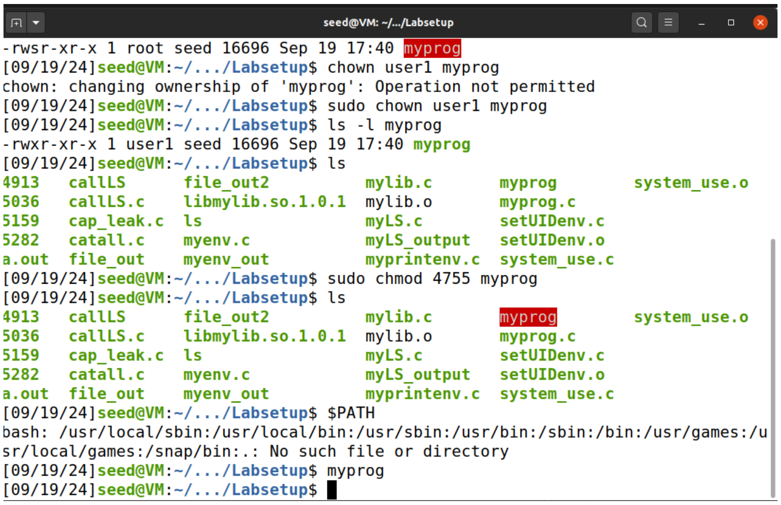
```
-rwxrwxrwx 1 seed seed 16784 Sep 16 00:19 ls
-rwxrwxrwx 1 seed seed   183 Sep 14 01:21 myenv.c
-rwxrwxrwx 1 seed seed 16824 Sep 14 01:22 myenv_out
-rwxrwxrwx 1 seed seed   150 Sep 19 16:57 mylib.c
-rw-rw-r-- 1 seed seed  5952 Sep 19 17:38 mylib.o
-rwxrwxrwx 1 seed seed    96 Sep 16 00:22 myLS.c
-rwxrwxrwx 1 seed seed   164 Sep 15 23:54 myLS_output
-rwxrwxrwx 1 seed seed   418 Sep 14 00:29 myprintenv.c
-rwxrwxr-x 1 seed seed 16696 Sep 19 17:40 myprog
-rwxrwxrwx 1 seed seed    71 Sep 19 17:01 myprog.c
-rwxrwxrwx 1 seed seed   153 Sep 14 02:38 setUIDenv.c
-rwxrwxrwx 1 seed seed 16768 Sep 14 02:38 setUIDenv.o
-rwxrwxrwx 1 seed seed    90 Sep 14 02:26 system_use.c
-rwxrwxrwx 1 seed seed 16704 Sep 14 02:27 system_use.o
[09/19/24]seed@VM:~/.../Labsetup$ sudo chown root myprog
[09/19/24]seed@VM:~/.../Labsetup$ ls -l | grep myprog
-rwxrwxr-x 1 root seed 16696 Sep 19 17:40 myprog
-rwxrwxrwx 1 seed seed    71 Sep 19 17:01 myprog.c
[09/19/24]seed@VM:~/.../Labsetup$ sudo chmod 4755 myprog
[09/19/24]seed@VM:~/.../Labsetup$ ls -l | grep myprog
-rwsr-xr-x 1 root seed 16696 Sep 19 17:40 myprog
-rwxrwxrwx 1 seed seed    71 Sep 19 17:01 myprog.c
[09/19/24]seed@VM:~/.../Labsetup$ myprog
[09/19/24]seed@VM:~/.../Labsetup$ 
```



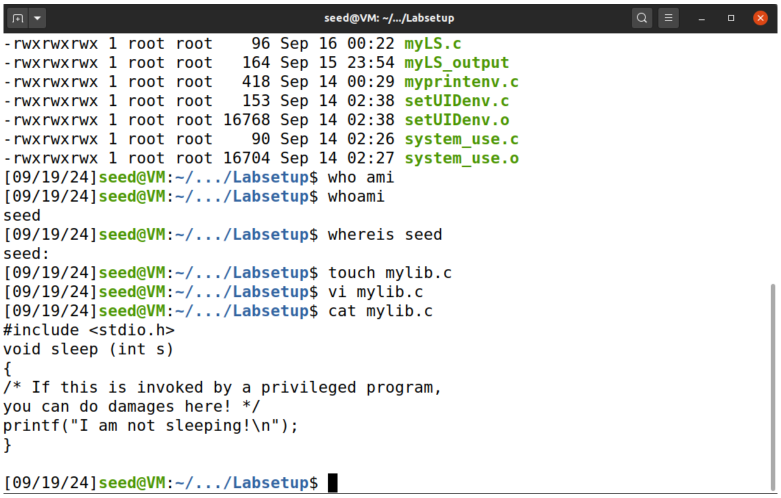
```
su: Authentication failure
[09/19/24]seed@VM:~/.../Labsetup$ su root
Password:
su: Authentication failure
[09/19/24]seed@VM:~/.../Labsetup$ sudo su
root@VM:/home/seed/Desktop/Labsetup# who ami
root@VM:/home/seed/Desktop/Labsetup#
root@VM:/home/seed/Desktop/Labsetup# whoami
root
root@VM:/home/seed/Desktop/Labsetup# export LD_PRELOAD=./libmylib.so.1.0.1
root@VM:/home/seed/Desktop/Labsetup# sudo su seed
[09/19/24]seed@VM:~/.../Labsetup$ myprog
[09/19/24]seed@VM:~/.../Labsetup$ sudo su
root@VM:/home/seed/Desktop/Labsetup# export LD_PRELOAD=./libmylib.so.1.0.1
root@VM:/home/seed/Desktop/Labsetup# myprog
myprog: command not found
root@VM:/home/seed/Desktop/Labsetup# ls
4913   callLS      file_out2          mylib.c       myprog        system_use.o
5036   callLS.c    libmylib.so.1.0.1  mylib.o       myprog.c
5159   cap_leak.c  ls                 myLS.c        setUIDenv.c
5282   catall.c    myenv.c            myLS_output   setUIDenv.o
a.out  file_out    myenv_out          myprintenv.c  system_use.c
root@VM:/home/seed/Desktop/Labsetup# myprog
myprog: command not found
```



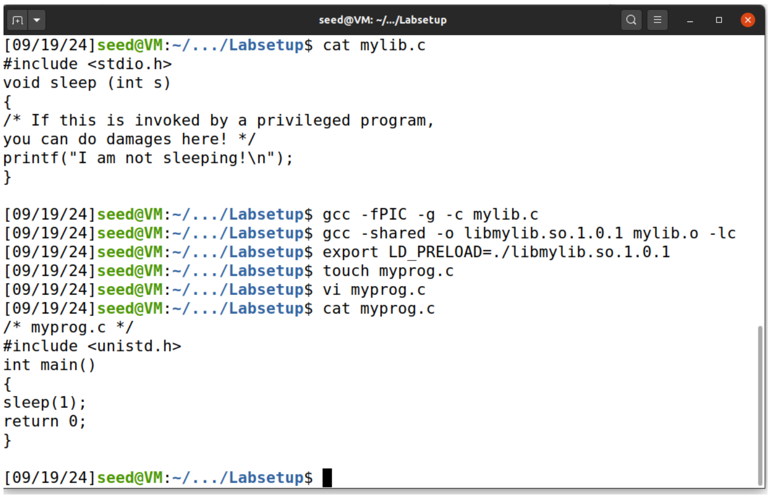
```
-rwsr-xr-x 1 root seed 16696 Sep 19 17:40 myprog
[09/19/24]seed@VM:~/.../Labsetup$ chown user1 myprog
chown: changing ownership of 'myprog': Operation not permitted
[09/19/24]seed@VM:~/.../Labsetup$ sudo chown user1 myprog
[09/19/24]seed@VM:~/.../Labsetup$ ls -l myprog
-rwxr-xr-x 1 user1 seed 16696 Sep 19 17:40 myprog
[09/19/24]seed@VM:~/.../Labsetup$ ls
4913   callLS      file_out2          mylib.c       myprog        syste
5036   callLS.c    libmylib.so.1.0.1  mylib.o       myprog.c
5159   cap_leak.c  ls                 myLS.c        setUIDenv.c
5282   catall.c    myenv.c            myLS_output   setUIDenv.o
a.out  file_out    myenv_out          myprintenv.c  system_use.c
[09/19/24]seed@VM:~/.../Labsetup$ sudo chmod 4755 myprog
[09/19/24]seed@VM:~/.../Labsetup$ ls
4913   callLS      file_out2          mylib.c       myprog        syste
5036   callLS.c    libmylib.so.1.0.1  mylib.o       myprog.c
5159   cap_leak.c  ls                 myLS.c        setUIDenv.c
5282   catall.c    myenv.c            myLS_output   setUIDenv.o
a.out  file_out    myenv_out          myprintenv.c  system_use.c
```



```
-rwsr-xr-x 1 root seed 16696 Sep 19 17:40 myprog
[09/19/24]seed@VM:~/.../Labsetup$ chown user1 myprog
chown: changing ownership of 'myprog': Operation not permitted
[09/19/24]seed@VM:~/.../Labsetup$ sudo chown user1 myprog
[09/19/24]seed@VM:~/.../Labsetup$ ls -l myprog
-rwxr-xr-x 1 user1 seed 16696 Sep 19 17:40 myprog
[09/19/24]seed@VM:~/.../Labsetup$ ls
4913   callLS      file_out2          mylib.c       myprog        system_use.o
5036   callLS.c    libmylib.so.1.0.1  mylib.o       myprog.c
5159   cap_leak.c  ls                 myLS.c        setUIDenv.c
5282   catall.c    myenv.c            myLS_output   setUIDenv.o
a.out  file_out    myenv_out          myprintenv.c  system_use.c
[09/19/24]seed@VM:~/.../Labsetup$ sudo chmod 4755 myprog
[09/19/24]seed@VM:~/.../Labsetup$ ls
4913   callLS      file_out2          mylib.c       myprog        system_use.o
5036   callLS.c    libmylib.so.1.0.1  mylib.o       myprog.c
5159   cap_leak.c  ls                 myLS.c        setUIDenv.c
5282   catall.c    myenv.c            myLS_output   setUIDenv.o
a.out  file_out    myenv_out          myprintenv.c  system_use.c
[09/19/24]seed@VM:~/.../Labsetup$ $PATH
bash: /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/u
sr/local/games:/snap/bin:.: No such file or directory
[09/19/24]seed@VM:~/.../Labsetup$ myprog
[09/19/24]seed@VM:~/.../Labsetup$ 
```



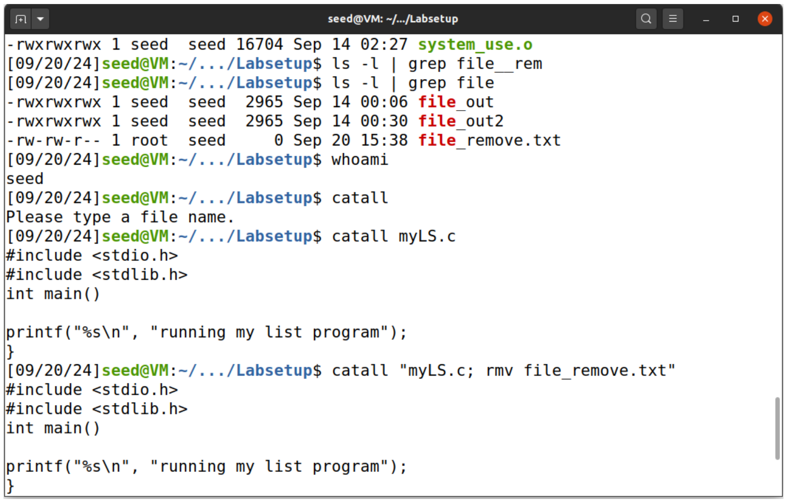
```
-rwxrwxrwx 1 root root    96 Sep 16 00:22 myLS.c
-rwxrwxrwx 1 root root   164 Sep 15 23:54 myLS_output
-rwxrwxrwx 1 root root   418 Sep 14 00:29 myprintenv.c
-rwxrwxrwx 1 root root   153 Sep 14 02:38 setUIDenv.c
-rwxrwxrwx 1 root root 16768 Sep 14 02:38 setUIDenv.o
-rwxrwxrwx 1 root root    90 Sep 14 02:26 system_use.c
-rwxrwxrwx 1 root root 16704 Sep 14 02:27 system_use.o
[09/19/24]seed@VM:~/.../Labsetup$ who ami
[09/19/24]seed@VM:~/.../Labsetup$ whoami
seed
[09/19/24]seed@VM:~/.../Labsetup$ whereis seed
seed:
[09/19/24]seed@VM:~/.../Labsetup$ touch mylib.c
[09/19/24]seed@VM:~/.../Labsetup$ vi mylib.c
[09/19/24]seed@VM:~/.../Labsetup$ cat mylib.c
#include <stdio.h>
void sleep (int s)
{
/* If this is invoked by a privileged program,
you can do damages here! */
printf("I am not sleeping!\n");
}

[09/19/24]seed@VM:~/.../Labsetup$ 
```



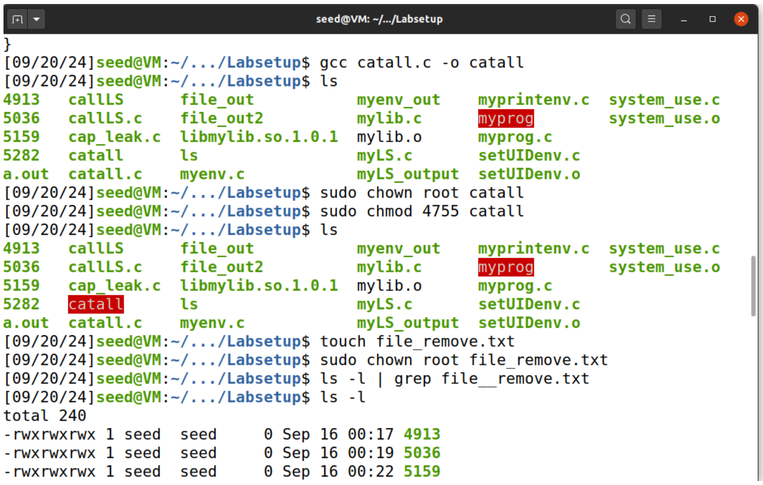
```
[09/19/24]seed@VM:~/.../Labsetup$ cat mylib.c
#include <stdio.h>
void sleep (int s)
{
/* If this is invoked by a privileged program,
you can do damages here! */
printf("I am not sleeping!\n");
}

[09/19/24]seed@VM:~/.../Labsetup$ gcc -fPIC -g -c mylib.c
[09/19/24]seed@VM:~/.../Labsetup$ gcc -shared -o libmylib.so.1.0.1 mylib.o -lc
[09/19/24]seed@VM:~/.../Labsetup$ export LD_PRELOAD=./libmylib.so.1.0.1
[09/19/24]seed@VM:~/.../Labsetup$ touch myprog.c
[09/19/24]seed@VM:~/.../Labsetup$ vi myprog.c
[09/19/24]seed@VM:~/.../Labsetup$ cat myprog.c
/* myprog.c */
#include <unistd.h>
int main()
{
sleep(1);
return 0;
}

[09/19/24]seed@VM:~/.../Labsetup$ 
```

Task 8:

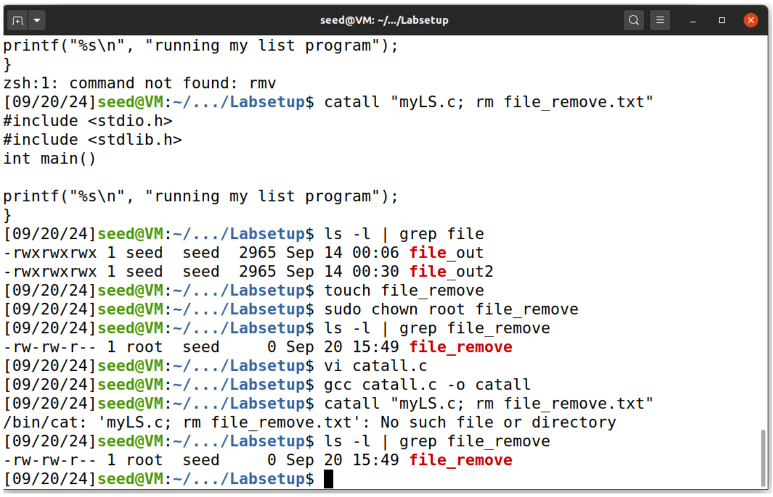
In our first step we are running our set uid program using system we run an extra command using this syntax “ arg1 ; command2” since our program does not separate data and code our system command runs the second command with the privileges set by the setuid program therefore having root privileges and can do things like modify file and or delete them. On on our second program we are running the execv() instead which actually differentiates between code and data so our file will try to run execv with whats in “” as the argument so the file try to cat a file with the whole name in the quotes and cat fine a file with that name so it errors.



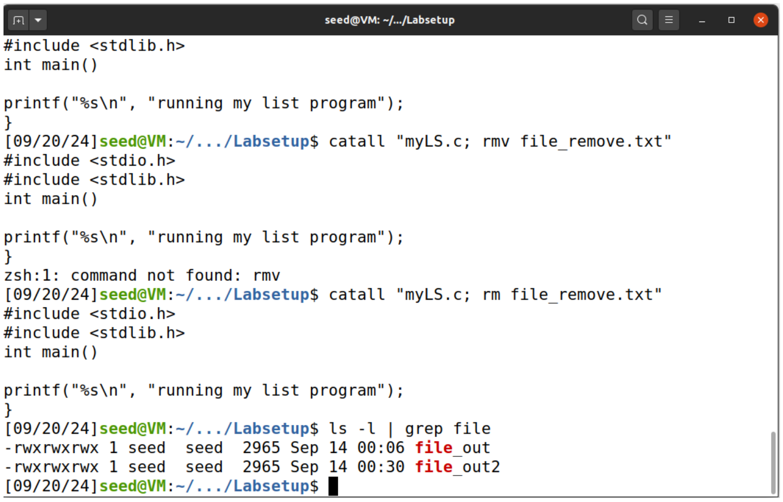
```
-rwxrwxrwx 1 seed  seed 16704 Sep 14 02:27 system_use.o
[09/20/24]seed@VM:~/.../Labsetup$ ls -l | grep file__rem
[09/20/24]seed@VM:~/.../Labsetup$ ls -l | grep file
-rwxrwxrwx 1 seed  seed  2965 Sep 14 00:06 file_out
-rwxrwxrwx 1 seed  seed  2965 Sep 14 00:30 file_out2
-rw-rw-r-- 1 root  seed     0 Sep 20 15:38 file_remove.txt
[09/20/24]seed@VM:~/.../Labsetup$ whoami
seed
[09/20/24]seed@VM:~/.../Labsetup$ catall
Please type a file name.
[09/20/24]seed@VM:~/.../Labsetup$ catall myLS.c
#include <stdio.h>
#include <stdlib.h>
int main()

printf("%s\n", "running my list program");
}
[09/20/24]seed@VM:~/.../Labsetup$ catall "myLS.c; rmv file_remove.txt"
#include <stdio.h>
#include <stdlib.h>
int main()

printf("%s\n", "running my list program");
}
```



```
}
[09/20/24]seed@VM:~/.../Labsetup$ gcc catall.c -o catall
[09/20/24]seed@VM:~/.../Labsetup$ ls
4913   callLS      file_out            myenv_out    myprintenv.c  system_use.c
5036   callLS.c    file_out2           mylib.c      myprog        system_use.o
5159   cap_leak.c  libmylib.so.1.0.1   mylib.o      myprog.c
5282   catall      ls                  myLS.c       setUIDenv.c
a.out  catall.c    myenv.c             myLS_output  setUIDenv.o
[09/20/24]seed@VM:~/.../Labsetup$ sudo chown root catall
[09/20/24]seed@VM:~/.../Labsetup$ sudo chmod 4755 catall
[09/20/24]seed@VM:~/.../Labsetup$ ls
4913   callLS      file_out            myenv_out    myprintenv.c  system_use.c
5036   callLS.c    file_out2           mylib.c      myprog        system_use.o
5159   cap_leak.c  libmylib.so.1.0.1   mylib.o      myprog.c
5282   catall      ls                  myLS.c       setUIDenv.c
a.out  catall.c    myenv.c             myLS_output  setUIDenv.o
[09/20/24]seed@VM:~/.../Labsetup$ touch file_remove.txt
[09/20/24]seed@VM:~/.../Labsetup$ sudo chown root file_remove.txt
[09/20/24]seed@VM:~/.../Labsetup$ ls -l | grep file__remove.txt
[09/20/24]seed@VM:~/.../Labsetup$ ls -l
total 240
-rwxrwxrwx 1 seed  seed     0 Sep 16 00:17 4913
-rwxrwxrwx 1 seed  seed     0 Sep 16 00:19 5036
-rwxrwxrwx 1 seed  seed     0 Sep 16 00:22 5159
```



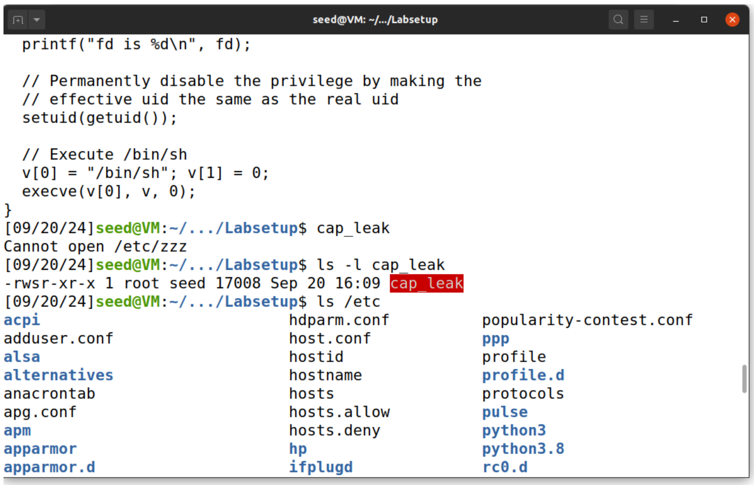
```
printf("%s\n", "running my list program");
}
zsh:1: command not found: rmv
[09/20/24]seed@VM:~/.../Labsetup$ catall "myLS.c; rm file_remove.txt"
#include <stdio.h>
#include <stdlib.h>
int main()

printf("%s\n", "running my list program");
}
[09/20/24]seed@VM:~/.../Labsetup$ ls -l | grep file
-rwxrwxrwx 1 seed  seed  2965 Sep 14 00:06 file_out
-rwxrwxrwx 1 seed  seed  2965 Sep 14 00:30 file_out2
[09/20/24]seed@VM:~/.../Labsetup$ touch file_remove
[09/20/24]seed@VM:~/.../Labsetup$ sudo chown root file_remove
[09/20/24]seed@VM:~/.../Labsetup$ ls -l | grep file_remove
-rw-rw-r-- 1 root  seed     0 Sep 20 15:49 file_remove
[09/20/24]seed@VM:~/.../Labsetup$ vi catall.c
[09/20/24]seed@VM:~/.../Labsetup$ gcc catall.c -o catall
[09/20/24]seed@VM:~/.../Labsetup$ catall "myLS.c; rm file_remove.txt"
/bin/cat: 'myLS.c; rm file_remove.txt': No such file or directory
[09/20/24]seed@VM:~/.../Labsetup$ ls -l | grep file_remove
-rw-rw-r-- 1 root  seed     0 Sep 20 15:49 file_remove
[09/20/24]seed@VM:~/.../Labsetup$ 
```



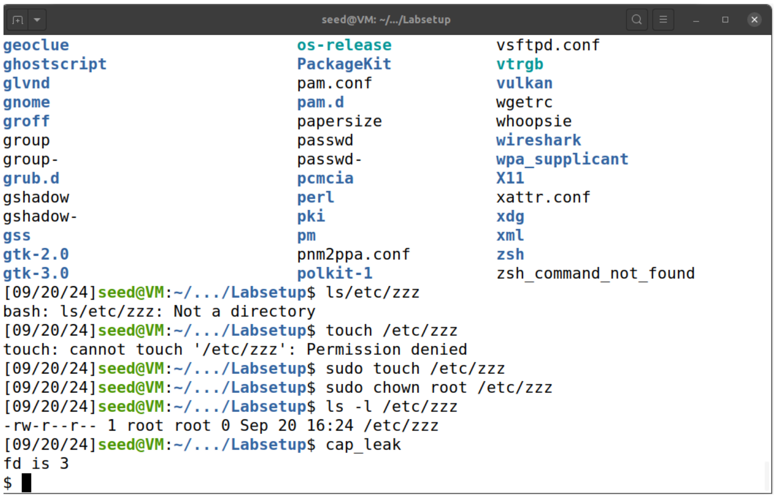
```
#include <stdlib.h>
int main()

printf("%s\n", "running my list program");
}
[09/20/24]seed@VM:~/.../Labsetup$ catall "myLS.c; rmv file_remove.txt"
#include <stdio.h>
#include <stdlib.h>
int main()

printf("%s\n", "running my list program");
}
zsh:1: command not found: rmv
[09/20/24]seed@VM:~/.../Labsetup$ catall "myLS.c; rm file_remove.txt"
#include <stdio.h>
#include <stdlib.h>
int main()

printf("%s\n", "running my list program");
}
[09/20/24]seed@VM:~/.../Labsetup$ ls -l | grep file
-rwxrwxrwx 1 seed  seed  2965 Sep 14 00:06 file_out
-rwxrwxrwx 1 seed  seed  2965 Sep 14 00:30 file_out2
[09/20/24]seed@VM:~/.../Labsetup$ 
```

Task 9:

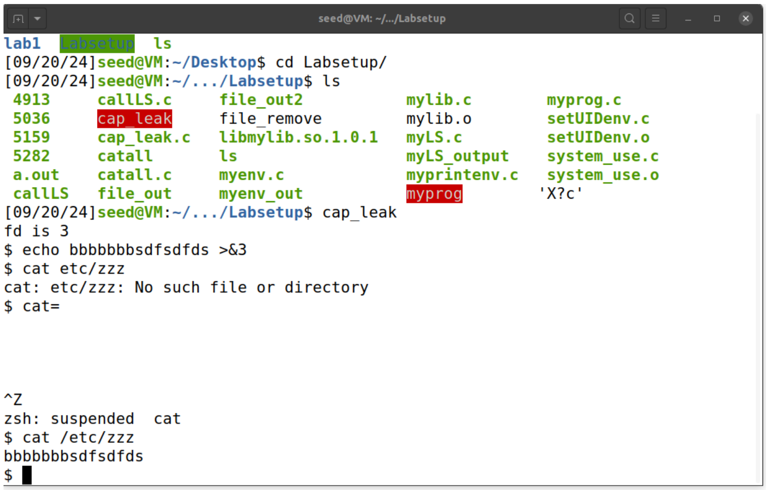
Yes we can exploit the capability by using the file descriptor from the file that wasn't closed to write to the file.



```
  printf("fd is %d\n", fd);

  // Permanently disable the privilege by making the
  // effective uid the same as the real uid
  setuid(getuid());

  // Execute /bin/sh
  v[0] = "/bin/sh"; v[1] = 0;
  execve(v[0], v, 0);
}
[09/20/24]seed@VM:~/.../Labsetup$ cap_leak
Cannot open /etc/zzz
[09/20/24]seed@VM:~/.../Labsetup$ ls -l cap_leak
-rwsr-xr-x 1 root seed 17008 Sep 20 16:09 cap_leak
[09/20/24]seed@VM:~/.../Labsetup$ ls /etc
acpi                           hdparm.conf          popularity-contest.conf
adduser.conf                   host.conf            ppp
alsa                           hostid               profile
alternatives                   hostname             profile.d
anacrontab                     hosts                protocols
apg.conf                       hosts.allow          pulse
apm                            hosts.deny           python3
apparmor                       hp                   python3.8
apparmor.d                     ifplugd              rc0.d
```



```
geoclue                        os-release           vsftpd.conf
ghostscript                    PackageKit           vtrgb
glvnd                          pam.conf             vulkan
gnome                          pam.d                wgetrc
groff                          papersize            whoopsie
group                          passwd               wireshark
group-                         passwd-              wpa_supplicant
grub.d                         pcmcia               X11
gshadow                        perl                 xattr.conf
gshadow-                       pki                  xdg
gss                            pm                   xml
gtk-2.0                        pnm2ppa.conf         zsh
gtk-3.0                        polkit-1             zsh_command_not_found
[09/20/24]seed@VM:~/.../Labsetup$ ls/etc/zzz
bash: ls/etc/zzz: Not a directory
[09/20/24]seed@VM:~/.../Labsetup$ touch /etc/zzz
touch: cannot touch '/etc/zzz': Permission denied
[09/20/24]seed@VM:~/.../Labsetup$ sudo touch /etc/zzz
[09/20/24]seed@VM:~/.../Labsetup$ sudo chown root /etc/zzz
[09/20/24]seed@VM:~/.../Labsetup$ ls -l /etc/zzz
-rw-r--r-- 1 root root 0 Sep 20 16:24 /etc/zzz
[09/20/24]seed@VM:~/.../Labsetup$ cap_leak
fd is 3
$ 
```



```
lab1  Labsetup  ls
[09/20/24]seed@VM:~/Desktop$ cd Labsetup/
[09/20/24]seed@VM:~/.../Labsetup$ ls
 4913     callLS.c     file_out2           mylib.c        myprog.c
 5036     cap_leak     file_remove         mylib.o        setUIDenv.c
 5159     cap_leak.c   libmylib.so.1.0.1   myLS.c         setUIDenv.o
 5282     catall       ls                  myLS_output    system_use.c
 a.out    catall.c     myenv.c             myprintenv.c   system_use.o
 callLS   file_out     myenv_out           myprog        'X?c'
[09/20/24]seed@VM:~/.../Labsetup$ cap_leak
fd is 3
$ echo bbbbbbbsdfsdfds >&3
$ cat etc/zzz
cat: etc/zzz: No such file or directory
$ cat=




^Z
zsh: suspended  cat
$ cat /etc/zzz
bbbbbbbsdfsdfds
$ 
```