Environment Variable and `Set-UID` Program Lab

57117213 张曙

Task 1: Manipulating Environment Variables

使用`printenv`打印环境变量

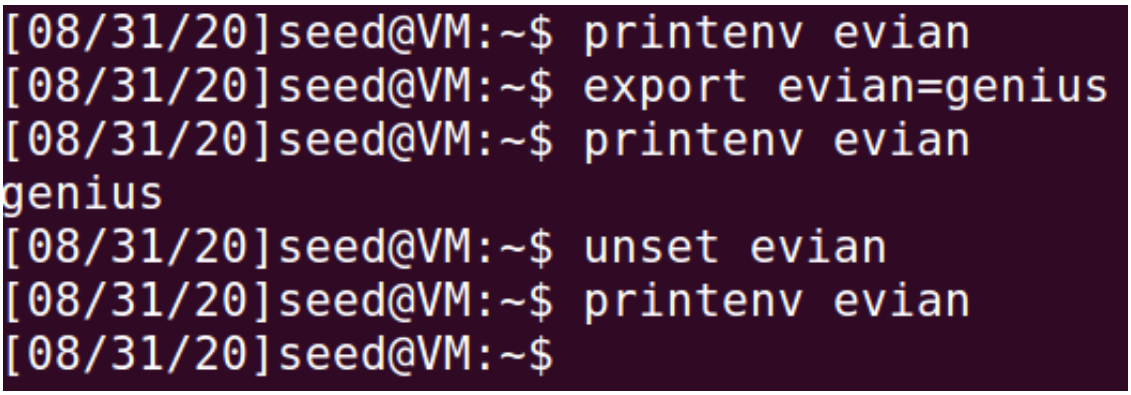
结果为

```
XDG_VTNR=7
XDG_SESSION_ID=c1
XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed
CLUTTER_IM_MODULE=xim
SESSION=ubuntu
ANDROID_HOME=/home/seed/android/android-sdk-linux
GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1
TERM=xterm-256color
VTE_VERSION=4205
XDG_MENU_PREFIX=gnome-
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/boost/libboost_system.s
o.1.64.0
WINDOWID=62914570
UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1396
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:*.l
ha=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:*.Z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01
;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.bz2=01;31:*.bz=01;31:*.tbz=01;31:*.tbz
2=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:*.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=0
1;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:*.fl
ac=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/boo
st_1_64_0/stage/lib:
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:/b
in:/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=unity-settings-daemon
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-lowgfx
IM_CONFIG_PHASE=1
GDMSESSION=ubuntu
SESSIONTYPE=gnome-session
```

```
GTK2_MODULES=overlay-scrollbar
SHLVL=1
HOME=/home/seed
XDG_SEAT=seat0
LANGUAGE=en_US
LIBGL_ALWAYS_SOFTWARE=1
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
UPSTART_INSTANCE=
UPSTART_EVENTS=xsession started
XDG_SESSION_DESKTOP=ubuntu
LOGNAME=seed
COMPIZ_BIN_PATH=/usr/bin/
DBUS_SESSION_BUS_ADDRESS=unix:abstract=/tmp/dbus-fJdXl82raq
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=
UPSTART_JOB=unity7
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
_=/usr/bin/printenv
```

使用`export`和`unset`设置和取消环境变量



如图：

1. 在设置之前，`printenv evian`的结果为空
2. 使用`export evian=genius`将`evian`环境变量的值设置为`genius`
3. 再次使用`printenv evian`，结果为`genius`
4. 使用`unset evian`，取消`evian`环境变量
5. 再次使用`printenv evian`，结果为空

Task2: Passing Environment Variables from Parent Process to Child Process

Step 1

注释掉`default`分支的`printenv`，保留`case 0`分支的`printenv`，即打印子进程的环境变量。其结果与Task 1结果完全一致（除了`_`环境变量为当前可执行程序名`./task_2`）。

将结果保存在`child_1`中：

```
./task_2 > child_1
```

Step 2

注释掉`case 0`分支的`printenv`，保留`default`分支的`printenv`，即打印父进程的环境变量。其结果与`Task 1`结果完全一致（除了`_`环境变量为当前可执行程序名`./task_2`）。

将结果保存在`child_2`中：

```
./task_2 > child_2
```

Step 3

使用`diff child_1 child_2`查看两个文件的差异，输出为空。即两次输出无差异。

结论

当我们使用`fork()`创建子进程的时候，子进程会自动继承父进程的所有环境变量，因此如果在程序内部不对环境变量进行修改，则父进程与子进程的环境变量应完全一致。

Task 3: Environment Variables and `execve()`

Step 1

将`NULL`作为第三个参数传给`execve`：

```
execve("/usr/bin/env", argv, NULL);
```

编译运行后输出为空。

Step 2

将外部变量`environ`作为第三个参数传给`execve`：

```
execve("/usr/bin/env", argv, environ);
```

编译运行后输出与Task 1完全一致（除了`_`环境变量为当前可执行程序名`task_3`）。

Step 3

结论：使用`execve()`创建的子进程，其环境变量完全取决于`execve()`的第三个参数。其第三个参数为一个字符串数组，每个元素是一个`char[]`类型字符串，代表其环境变量。

Task 4: Environment Variables and `system()`

使用`system("/usr/bin/env")`后，输出与Task 1完全一致（除了`_`环境变量为当前可执行程序名`./task_4`）。

说明使用`system()`创建子进程时会继承父进程的所有环境变量。

Task 5: Environment Variable and `Set-UID` Programs

Step 1

逐行打印当前的环境变量，可执行程序为普通可执行程序，用户为一般用户，输出结果与Task 1完全一致（除了`_`环境变量为当前可执行程序名`./task_5`）。

Step 2

使用

```
sudo chown root task_5
sudo chmod 4755 task_5
```

将程序变为`root`用户的`Set-UID`程序。

Step 3

在普通用户的Shell下，使用`export`命令设置：

- `PATH`
- `LD_LIBRARY_PATH`
- 任何名称（我设置为`GENIUS=evian`）

```
[08/31/20]seed@VM:~$ export PATH=evian
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=evian
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 GENIUS=evian
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
```

（这里的报错应该是这个终端的Prompt中用`date`命令获取了当前的时间，然后我把`PATH`设置成了别的路径，就找不到这个程序了）

以普通用户身份运行在Step 2中编译的程序，输出为：

```
CLUTTER_IM_MODULE=xim
SESSION=ubuntu
ANDROID_HOME=/home/seed/android/android-sdk-linux
GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1
TERM=xterm-256color
VTE_VERSION=4205
XDG_MENU_PREFIX=gnome-
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/boost/libboost_system.s
o.1.64.0
WINDOWID=62914570
OLDPWD=/home/seed/Downloads
UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1396
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:*.l
ha=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:*.Z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01
;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.bz2=01;31:*.bz=01;31:*.tbz=01;31:*.tbz
2=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:*.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=0
1;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:*.fl
ac=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/boo
st_1_64_0/stage/lib:
XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0
XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
GENIUS=evian
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=evian
QT_IM_MODULE=ibus
QT_QPA_PLATFORMTHEME=appmenu-qt5
XDG_SESSION_TYPE=x11
PWD=/home/seed
JOB=unity-settings-daemon
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-lowgfx
IM_CONFIG_PHASE=1
GDMSESSION=ubuntu
SESSIONTYPE=gnome-session
GTK2_MODULES=overlay-scrollbar
SHLVL=1
HOME=/home/seed
XDG_SEAT=seat0
```

```
LANGUAGE=en_US
LIBGL_ALWAYS_SOFTWARE=1
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
UPSTART_INSTANCE=
UPSTART_EVENTS=xsession started
XDG_SESSION_DESKTOP=ubuntu
LOGNAME=seed
COMPIZ_BIN_PATH=/usr/bin/
DBUS_SESSION_BUS_ADDRESS=unix:abstract=/tmp/dbus-fJdXl82raq
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=
UPSTART_JOB=unity7
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
_=./task_5
```

可以看到这里面`PATH`变成了`evian`，`GENIUS`变成了`evian`，但是`LD_LIBRARY_PATH`却没有变。

经过搜索，`Set-UID`程序会自动忽略`LD_LIBRARY_PATH`环境变量。这是因为，这个环境变量控制的是程序的动态链接路径，如果不忽略，攻击者可以自己设置这个环境变量之后，使用`Set-UID`程序链接自己的动态链接库，造成极大破坏。

Task 6: The `PATH` Environment Variable and `Set-UID` Programs

首先使用

```
sudo ln -sf /bin/zsh /bin/sh
```

将`/bin/sh`链接到`/bin/zsh`上。

然后将当前的home路径添加到`PATH`中：

```
export PATH=/home/seed:$PATH
```

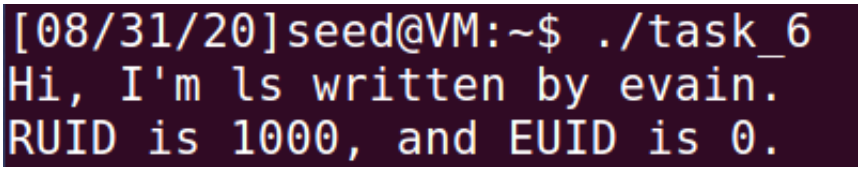
接着，在`/home/seed`目录下编写`ls.c`：

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

int main() {
    printf("Hi, I'm ls written by evain.\nRUID is %d, and EUID is %d.\n",
getuid(), geteuid());
    return 0;
}
```

并编译为`ls`程序。

然后将给出的代码编译为`task_6`程序，并使之成为root的`Set-UID`程序，运行：



成功调用了我们自己写的程序。同时也可以观察到，此时Real user ID为1000，也就是当前普通用户seed的uid，而Effective user ID为0，也就是root的uid。

解释

首先，我们调用`task_6`程序时，会自动继承我们当前的环境变量，所以此时`PATH`包含`/home/seed`，并且优先级最高。当我们使用相对路径调用`ls`时，系统会首先在`PATH`中寻找，那么就会第一个找到`/home/seed/ls`，因此可以调用我们的程序。

同时，使用`system()`创建的子进程的RUID与EUID和父进程一致，所以我们的程序可以以root权限运行。

Task 7: The `LD_PRELOAD` Environment Variable and `Set-UID` Programs

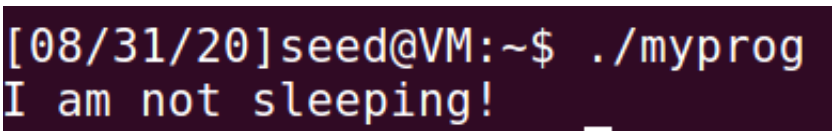
Step 1

在当前目录下编译动态链接库`libmylib.so.1.0.1`，里面有`sleep`函数。

将`LD_PRELOAD`设置为我们编译的动态链接库。

Step 2

普通用户运行普通程序`myprog`



说明`sleep`是`libmylib.so.1.0.1`的。

普通用户运行`Set-UID`的root程序`myprog`

```
[08/31/20]seed@VM:~$ sudo chown root ./myprog
[08/31/20]seed@VM:~$ sudo chmod 4755 ./myprog
[08/31/20]seed@VM:~$ ./myprog
[08/31/20]seed@VM:~$
```

说明`sleep`是系统库的。

root用户设置好`LD_PRELOAD`后运行`Set-UID`的root程序`myprog`

```
root@VM:/home/seed# export LD_PRELOAD=./libmylib.so.1.0.1
root@VM:/home/seed# ./myprog
I am not sleeping!
```

说明`sleep`是`libmylib.so.1.0.1`的。

当前用户运行`Set-UID`的别的普通用户程序`myprog`

```
[08/31/20]seed@VM:~$ sudo chown evian ./myprog
[08/31/20]seed@VM:~$ sudo chmod 4755 ./myprog
[08/31/20]seed@VM:~$ ./myprog
[08/31/20]seed@VM:~$
```

说明`sleep`是系统库的。

Step 3

当RUID与EUID一致时，`Set-UID`程序会识别`LD_PRELOAD`环境变量；当其不一致时，`Set-UID`程序会忽略这一变量。

验证：

```c
int main() {
    system("env | grep LD_PRELOAD");
    return 0;
}
```

将上述程序编写并编译为`task_7`程序。

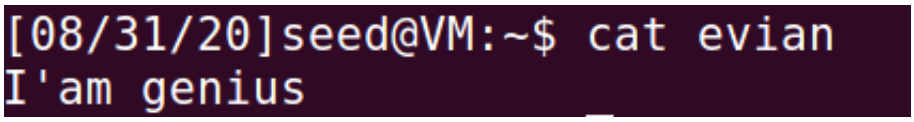
- 普通用户运行普通程序
  将`LD_PRELOAD`设置为`evian`，运行`task_7`后输出`LD_PRELOAD=evian`。
- 普通用户运行root的`Set-UID`程序
  将`LD_PRELOAD`设置为`evian`，运行后`task_7`输出为空
- root用户运行root的`Set-UID`程序
  root权限下将`LD_PRELOAD`设置为`evian`，运行`task_7`后输出`LD_PRELOAD=evian`。
- 普通用户运行别的普通用户的`Set-UID`程序
  将`LD_PRELOAD`设置为`evian`，运行`task_7`输出为空

以上四个验证说明，只有当RUID与EUID一致时，才会继承`LD_PRELOAD`环境变量。

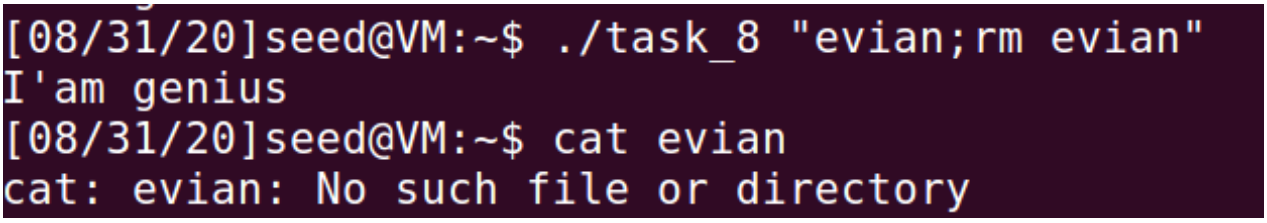
Task 8: Invoking External Programs Using `system()` versus `execve()`

Step 1

首先，我们创建一个`evian`文件，内容为"I'am genius"。



调用时输入加上`;`来增加一行调用：



在打印了`evian`文件的内容之后，`evian`文件被删除了。

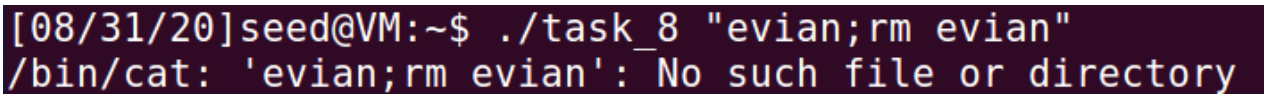
这是因为，当我们的输入为`evian; rm evian`时，程序实际上执行的`command`是：

```
/bin/cat evian; rm evian
```

也就是执行了两个指令。

Step 2

将`system()`指令换成`execve()`指令后，再次进行这一操作：

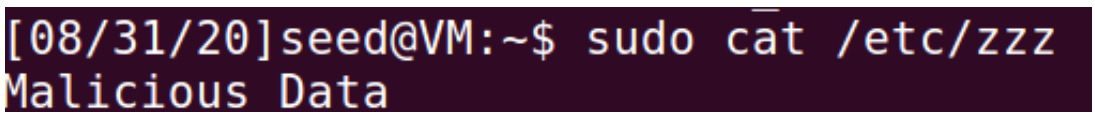


失败，这是因为，`execve()`只执行名字为其第一个参数的子程序，将第二个参数"evian;rm evian"作为参数传递给子程序，所以子程序实际上是查看`evian;rm evian`这个文件，其不存在。

总结而言，就是`system()`不能分辨指令和数据，而`execve()`的指令是其第一个参数，数据是其第二个参数。

Task 9: Capability Leaking

首先创建`/etc/zzz`文件。然后，按照题目指令运行相应的程序后，查看`/etc/zzz`文件：



发现确实能够写入。

这是因为，在调用`fork()`之前，`fd`并没有被关闭，因此，子进程会复制父进程所有的文件描述符，也包括`fd`。在父进程中，使用`close(fd)`关闭了`fd`，但是在子进程中由于是复制的，所以`fd`不受父进程影响，依然存在。此时，尽管子进程的权限已经被降级，但其拥有文件描述符，就可以对其进行修改，从而对`/etc/zzz`文件进行了写操作。