实验0：Environment Variable and Set-UID Program

# Task 1: Manipulating Environment Variables

① 打印环境变量

[09/01/20]seed@VM:~$ printenv

XDG\_VTNR=7

LC\_PAPER=zh\_CN.UTF-8

ORBIT\_SOCKETDIR=/tmp/orbit-seed

LC\_ADDRESS=zh\_CN.UTF-8

XDG\_SESSION\_ID=c1

XDG\_GREETER\_DATA\_DIR=/var/lib/lightdm-data/seed

IBUS\_DISABLE\_SNOOPER=1

TERMINATOR\_UUID=urn:uuid:d454cc9b-7cdb-4a1f-8cd6-79f80fa96f29

LC\_MONETARY=zh\_CN.UTF-8

CLUTTER\_IM\_MODULE=xim

SESSION=ubuntu

GIO\_LAUNCHED\_DESKTOP\_FILE\_PID=3459

ANDROID\_HOME=/home/seed/android/android-sdk-linux

GPG\_AGENT\_INFO=/home/seed/.gnupg/S.gpg-agent:0:1

XDG\_MENU\_PREFIX=gnome-

SHELL=/bin/bash

TERM=xterm

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.so.1.64.0

WINDOWID=56623108

LC\_NUMERIC=zh\_CN.UTF-8

UPSTART\_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1476

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:\*.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:\*.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:\*.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:\*.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:

LC\_TELEPHONE=zh\_CN.UTF-8

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\_SOCK=/run/user/1000/keyring/ssh

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

SESSION\_MANAGER=local/VM:@/tmp/.ICE-unix/1761,unix/VM:/tmp/.ICE-unix/1761

GIO\_LAUNCHED\_DESKTOP\_FILE=/usr/share/applications/terminator.desktop

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

LC\_IDENTIFICATION=zh\_CN.UTF-8

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=zh\_CN.UTF-8

GDM\_LANG=zh\_CN

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

LC\_MEASUREMENT=zh\_CN.UTF-8

COMPIZ\_CONFIG\_PROFILE=ubuntu-lowgfx

IM\_CONFIG\_PHASE=1

PAPERSIZE=a4

GDMSESSION=ubuntu

SESSIONTYPE=gnome-session

GTK2\_MODULES=overlay-scrollbar

SHLVL=1

HOME=/home/seed

XDG\_SEAT=seat0

LANGUAGE=zh\_CN:en\_US:en

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-2i6JdeXqci

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

LC\_TIME=zh\_CN.UTF-8

LC\_NAME=zh\_CN.UTF-8

XAUTHORITY=/home/seed/.Xauthority

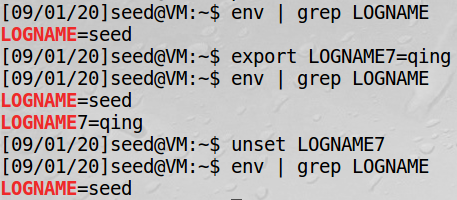
COLORTERM=gnome-terminal

\_=/usr/bin/printenv

[09/01/20]seed@VM:~$ printenv PWD

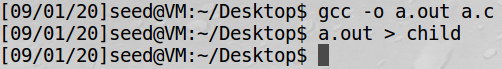
/home/seed

② 设置和取消环境变量

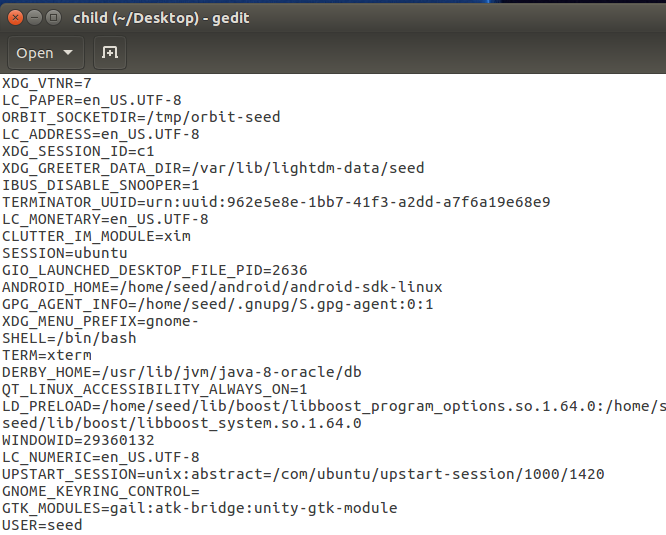


# Task 2: Passing Environment Variables from Parent Process to Child Process

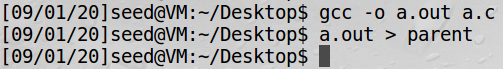
① 编译并运行程序，将结果输出到child



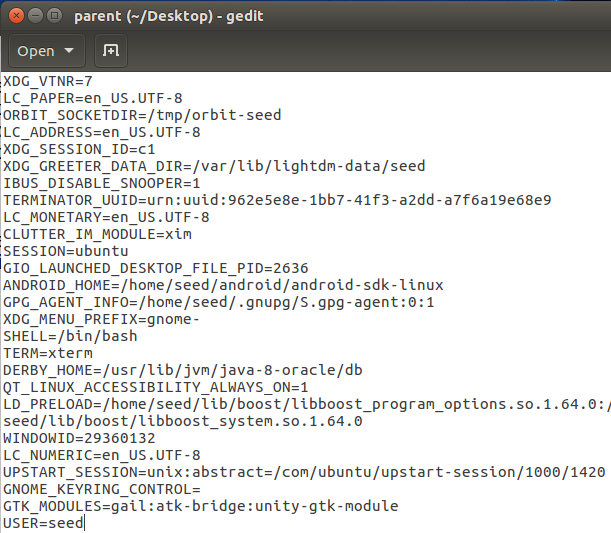
child文件中是子进程的环境变量



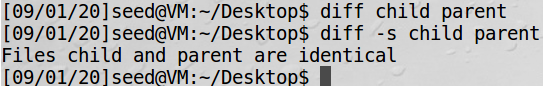
② 将第一个printenv()注释掉，取消第二个printenv()的注释，重新编译运行，结果输出到parent



parent文件中是父进程的环境变量



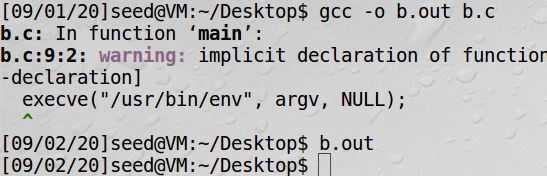
③ 比较两文件的不同



child和parent文件内容相同，说明子进程会继承父进程的环境变量

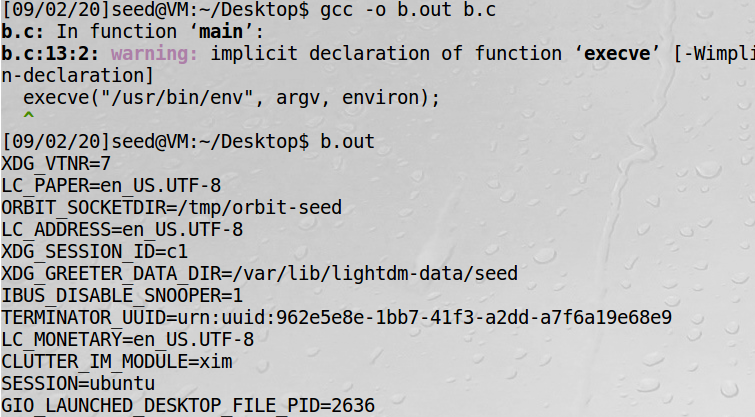
# Task 3: Environment Variables and execve()

① 编译并运行程序



没有输出

② 将execve("/usr/bin/env", argv, NULL)改为execve("/usr/bin/env", argv, environ)重新编译执行

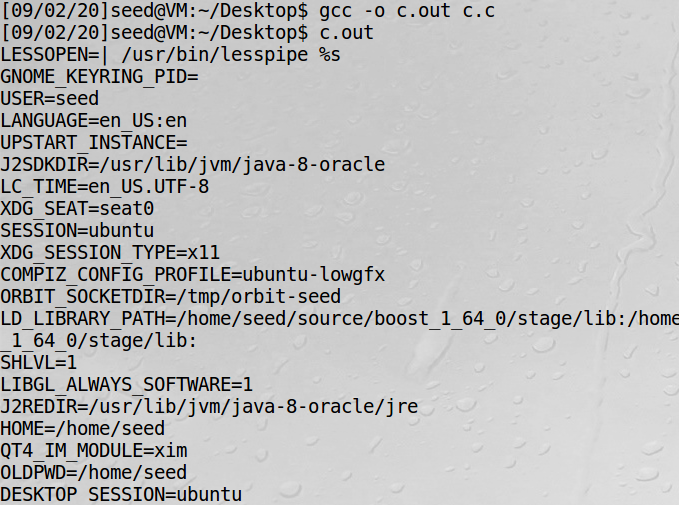


打印出环境变量

③ 结论：当调用execve()执行新的程序时，内存空间被覆盖，原来的环境变量不会自动继承到新的程序，需要通过execve()的第三个参数进行传递

# Task 4: Environment Variables and system()

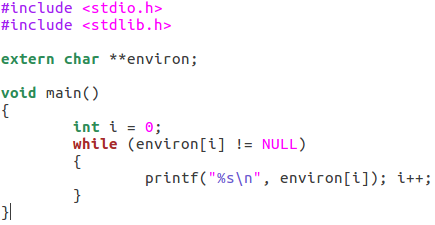
编译并执行程序



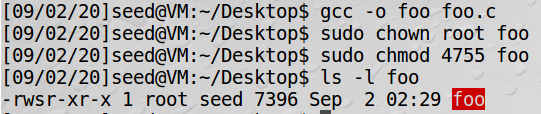
使用system()时，调用者进程的环境变量传递给了新程序/bin/sh

# Task 5: Environment Variable and Set-UID Programs

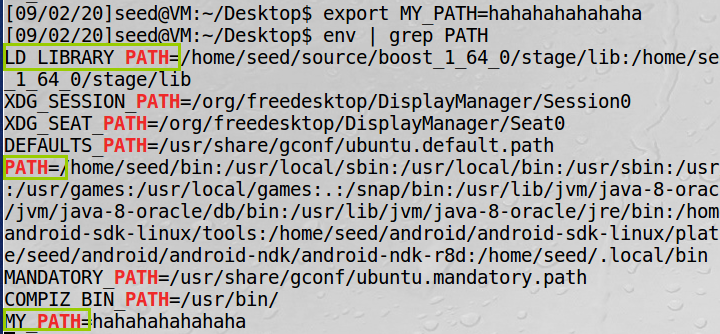
① 编译程序，生成可执行文件foo.out，该程序可打印当前进程的所有环境变量



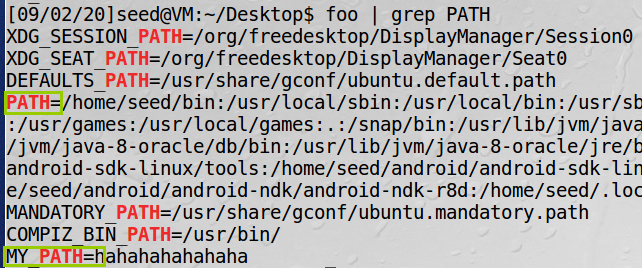
② 将程序的所有者改为root，并使其成为一个Set-UID程序



③ 在父进程中设置环境变量，观察Set-UID子进程中的环境变量

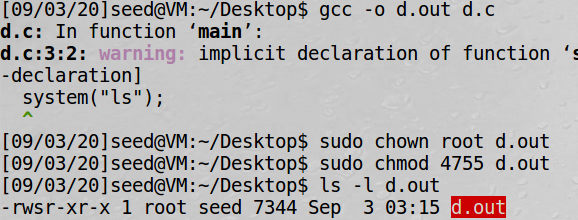


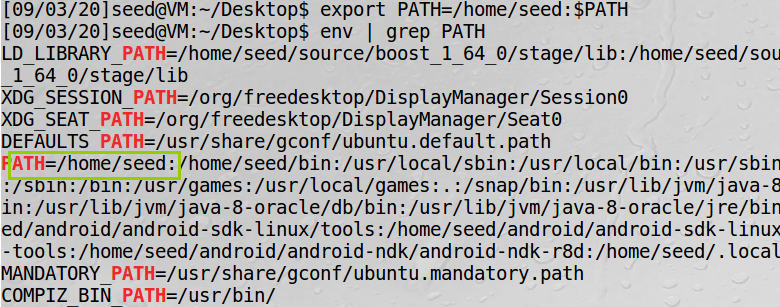
在父进程中，LD\_LIBRARY\_PATH、PATH、MY\_PATH三个环境变量都在



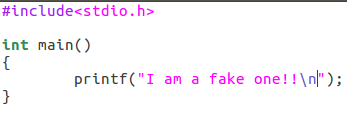
在子进程中，只有PATH、MY\_PATH这两个环境变量，LD\_LIBRARY\_PATH没有

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

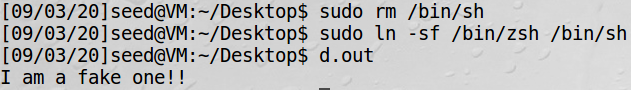




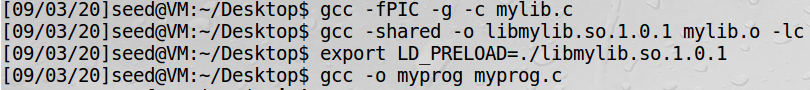
在/home/seed目录下放一个假的ls



将/bin/sh连接到zsh，运行d.out，发现执行的是假的ls，是以root权限运行的



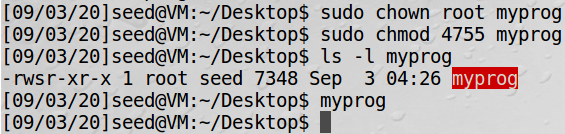
# Task 7: The LD\_PRELOAD Environment Variable and Set-UID Programs



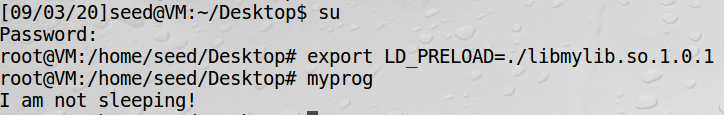
当myprog为普通程序，在普通用户下运行时，发现我们自己定义的库函数sleep被调用了



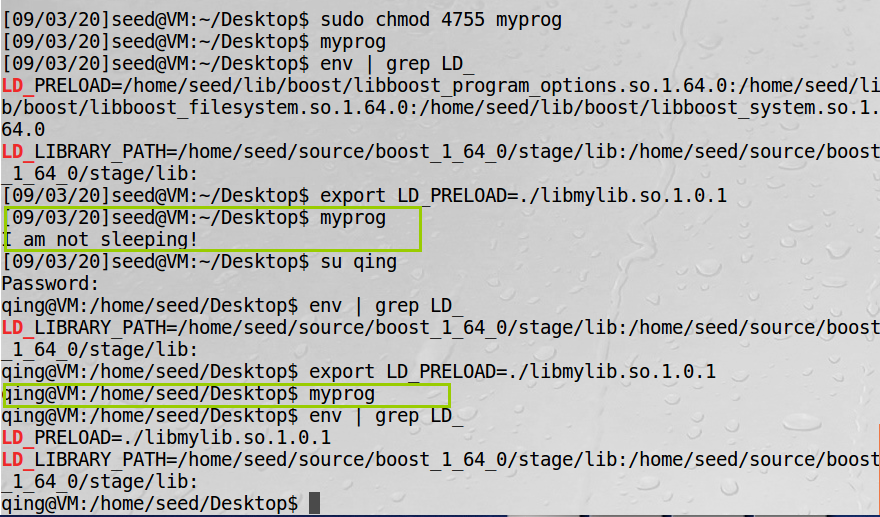
当myprog为set-uid root程序，在普通用户下运行时，运行的是系统的sleep



当myprog为set-uid root程序，在root用户下运行时，运行的是自己定义的sleep



将myprog的所有者改为seed，在另一个用户下（qing）运行它，运行的是系统的sleep



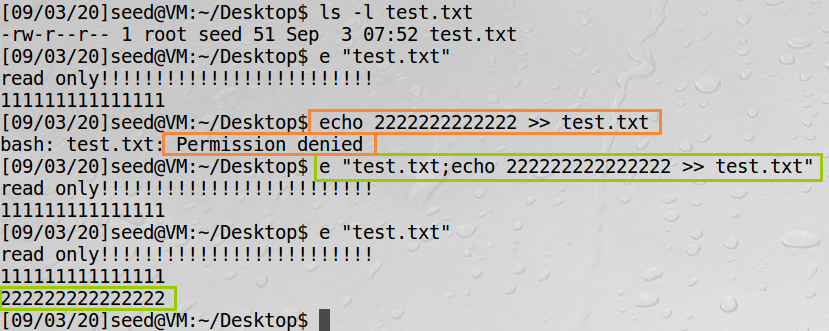
当EUID和RUID不同时，动态链接会忽略LD\_PRELOAD和LD\_LIBRARY\_PATH环境变量，相同时才有效。

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

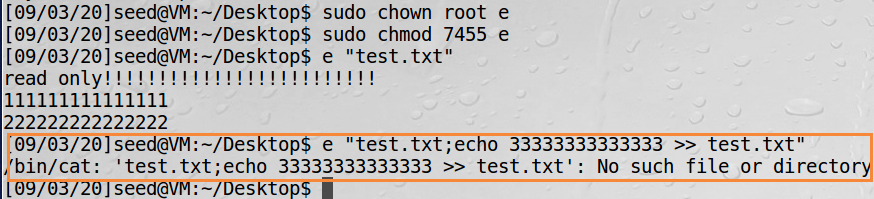
① 用system()不安全

有文件test.txt，他的所有者为root，只有root有权限写入

但攻击者依然可以向test中写入新的内容



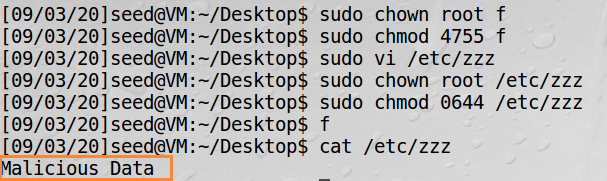
② 用execve()后攻击失效



execve()将“test.txt;echo 33333333333333 >> test.txt”这一整个部分视为函数的参数（文件名），不会像system()那样将分号后的部分当作命令

# Task 9: Capability Leaking

文件/etc/zzz被修改了



原因在于没有在降级前将fd关闭