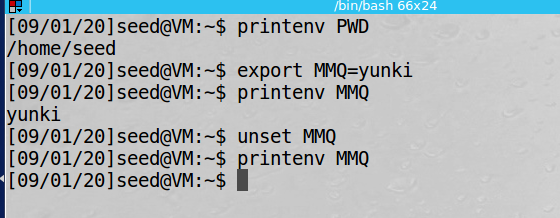
任务一：



任务二：

父进程环境变量：

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:aa9df58b-b599-40e9-bb2e-4611135eec97  
IBUS\_DISABLE\_SNOOPER=1  
CLUTTER\_IM\_MODULE=xim  
SESSION=ubuntu  
GIO\_LAUNCHED\_DESKTOP\_FILE\_PID=6251  
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/boost/libboost\_system.so.1.64.0  
WINDOWID=31457284  
UPSTART\_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1318  
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:  
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  
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  
XDG\_SESSION\_TYPE=x11  
PWD=/home/seed/Desktop  
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  
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=xsession started  
LOGNAME=seed  
COMPIZ\_BIN\_PATH=/usr/bin/  
DBUS\_SESSION\_BUS\_ADDRESS=unix:abstract=/tmp/dbus-qH1hoLz7qM  
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  
COLORTERM=gnome-terminal  
OLDPWD=/home/seed  
\_=./a.out

子进程环境变量：

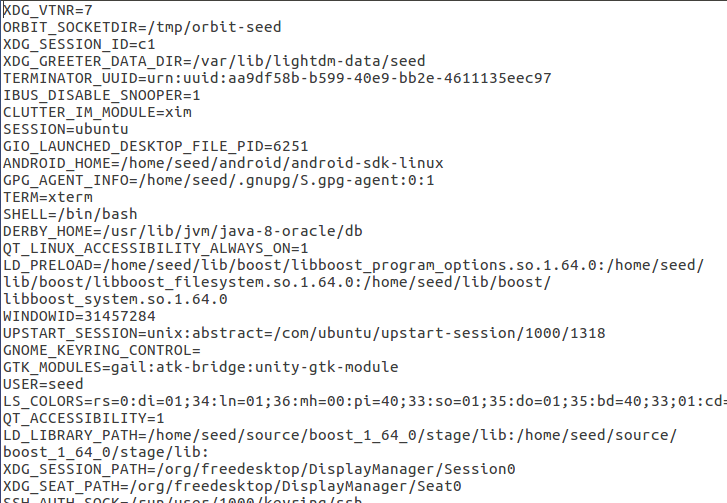
XDG\_VTNR=7  
ORBIT\_SOCKETDIR=/tmp/orbit-seed  
XDG\_SESSION\_ID=c1  
XDG\_GREETER\_DATA\_DIR=/var/lib/lightdm-data/seed  
TERMINATOR\_UUID=urn:uuid:aa9df58b-b599-40e9-bb2e-4611135eec97  
IBUS\_DISABLE\_SNOOPER=1  
CLUTTER\_IM\_MODULE=xim  
SESSION=ubuntu  
GIO\_LAUNCHED\_DESKTOP\_FILE\_PID=6251  
ANDROID\_HOME=/home/seed/android/android-sdk-linux  
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/boost/libboost\_system.so.1.64.0  
WINDOWID=31457284  
UPSTART\_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1318  
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:  
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  
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  
XDG\_SESSION\_TYPE=x11  
PWD=/home/seed/Desktop  
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  
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=xsession started  
LOGNAME=seed  
COMPIZ\_BIN\_PATH=/usr/bin/  
DBUS\_SESSION\_BUS\_ADDRESS=unix:abstract=/tmp/dbus-qH1hoLz7qM  
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  
COLORTERM=gnome-terminal  
OLDPWD=/home/seed  
\_=./a.out



Diff命令无输出，没有不同

任务三：

当execve中第三个参数为空时，新的进程环境变量也为空。当用environ遍历当前进程环境变量时，新的进程环境变量不为空：

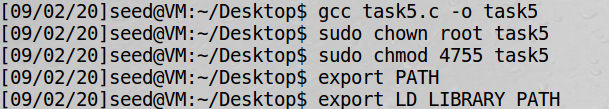


结论：环境变量不会被自动继承，而是通过参数传递

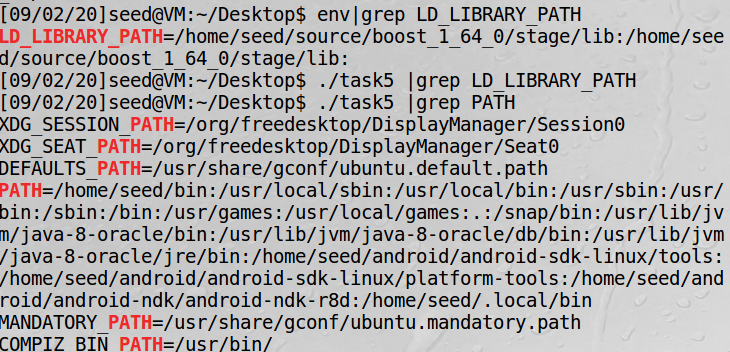
任务四：  
LESSOPEN=| /usr/bin/lesspipe %s  
GNOME\_KEYRING\_PID=  
USER=seed  
LANGUAGE=en\_US  
UPSTART\_INSTANCE=  
J2SDKDIR=/usr/lib/jvm/java-8-oracle  
XDG\_SEAT=seat0  
SESSION=ubuntu  
XDG\_SESSION\_TYPE=x11  
COMPIZ\_CONFIG\_PROFILE=ubuntu  
ORBIT\_SOCKETDIR=/tmp/orbit-seed  
LD\_LIBRARY\_PATH=/home/seed/source/boost\_1\_64\_0/stage/lib:/home/seed/source/boost\_1\_64\_0/stage/lib:  
SHLVL=1  
J2REDIR=/usr/lib/jvm/java-8-oracle/jre  
HOME=/home/seed  
QT4\_IM\_MODULE=xim  
OLDPWD=/home/seed  
DESKTOP\_SESSION=ubuntu  
GIO\_LAUNCHED\_DESKTOP\_FILE=/usr/share/applications/terminator.desktop  
QT\_LINUX\_ACCESSIBILITY\_ALWAYS\_ON=1  
GTK\_MODULES=gail:atk-bridge:unity-gtk-module  
XDG\_SEAT\_PATH=/org/freedesktop/DisplayManager/Seat0  
INSTANCE=  
DBUS\_SESSION\_BUS\_ADDRESS=unix:abstract=/tmp/dbus-8Om0llhjGA  
GIO\_LAUNCHED\_DESKTOP\_FILE\_PID=5712  
COLORTERM=gnome-terminal  
GNOME\_KEYRING\_CONTROL=  
QT\_QPA\_PLATFORMTHEME=appmenu-qt5  
MANDATORY\_PATH=/usr/share/gconf/ubuntu.mandatory.path  
IM\_CONFIG\_PHASE=1  
SESSIONTYPE=gnome-session  
UPSTART\_JOB=unity7  
LOGNAME=seed  
GTK\_IM\_MODULE=ibus  
WINDOWID=54525956  
\_=./a.out  
DEFAULTS\_PATH=/usr/share/gconf/ubuntu.default.path  
XDG\_SESSION\_ID=c1  
TERM=xterm  
GNOME\_DESKTOP\_SESSION\_ID=this-is-deprecated  
GTK2\_MODULES=overlay-scrollbar  
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  
DERBY\_HOME=/usr/lib/jvm/java-8-oracle/db  
GDM\_LANG=en\_US  
XDG\_SESSION\_PATH=/org/freedesktop/DisplayManager/Session0  
XDG\_RUNTIME\_DIR=/run/user/1000  
COMPIZ\_BIN\_PATH=/usr/bin/  
DISPLAY=:0  
IBUS\_DISABLE\_SNOOPER=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  
LANG=en\_US.UTF-8  
XDG\_CURRENT\_DESKTOP=Unity  
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:  
XMODIFIERS=@im=ibus  
XDG\_SESSION\_DESKTOP=ubuntu  
XAUTHORITY=/home/seed/.Xauthority  
XDG\_GREETER\_DATA\_DIR=/var/lib/lightdm-data/seed  
SSH\_AUTH\_SOCK=/run/user/1000/keyring/ssh  
TERMINATOR\_UUID=urn:uuid:8b0047c7-752c-4c87-bc88-fe0849b2fb4e  
SHELL=/bin/bash  
QT\_ACCESSIBILITY=1  
GDMSESSION=ubuntu  
LESSCLOSE=/usr/bin/lesspipe %s %s  
UPSTART\_EVENTS=xsession started  
GPG\_AGENT\_INFO=/home/seed/.gnupg/S.gpg-agent:0:1  
UPSTART\_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1623  
XDG\_VTNR=7  
QT\_IM\_MODULE=ibus  
PWD=/home/seed/Desktop  
JAVA\_HOME=/usr/lib/jvm/java-8-oracle  
CLUTTER\_IM\_MODULE=xim  
ANDROID\_HOME=/home/seed/android/android-sdk-linux  
XDG\_CONFIG\_DIRS=/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg  
XDG\_DATA\_DIRS=/usr/share/ubuntu:/usr/share/gnome:/usr/local/share/:/usr/share/:/var/lib/snapd/desktop  
JOB=unity-settings-daemon

结论：system不直接使用command，通过execl()运行shell，可以直接传递环境变量

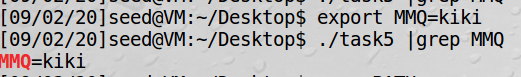
任务五：

修改程序权限及环境变量：  


Shell process中的LD\_LIBRARY\_PATH环境变量并未被child process继承，但PATH环境变量被继承

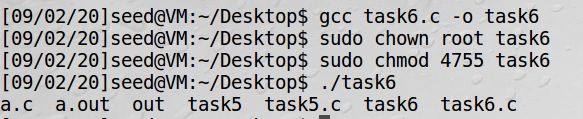


增加自定义环境变量，并发现自定义环境变量被child process继承



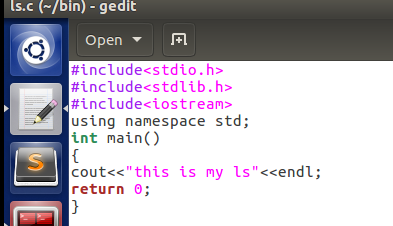
结论：会传递给子进程的两种shell变量：所有从环境变量中得到的shell变量（当一个shell程序启动时，为每个环境变量作一个拷贝，作为其shell变量）以及用户使用export自定义的shell变量

任务六：  
编译程序并修改程序特权后运行：

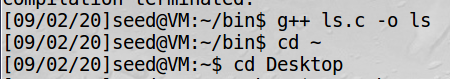


此时运行的是原有路径（root/bin）下的ls命令

在/home/bin 目录下增加自己定义的ls程序



编译ls程序：

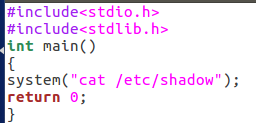


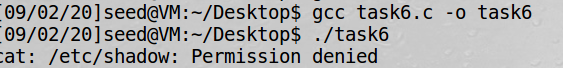
重新运行测试程序



此时运行的是自己编写的ls程序

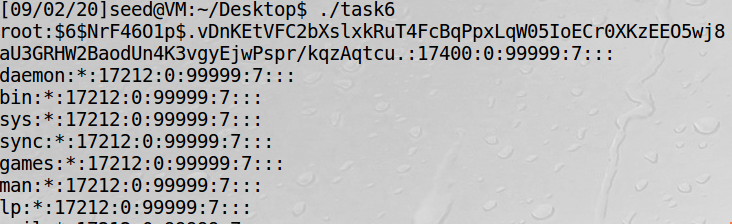
Note：  
ubuntu 16.04 VM：对setuid程序自动降级，无法实现特权指令：





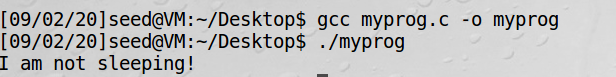
初始化shell程序zsh并将/bin/sh链接到zsh：



Setuid程序中特权指令可以被执行：  


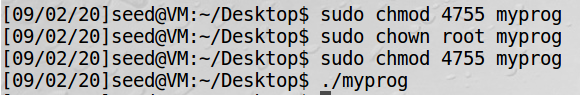
任务七：

1、普通程序，普通用户态：运行自定义函数



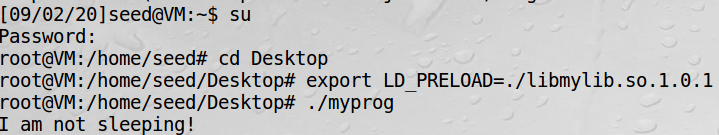
分析：shell中用户自定义的环境变量传递给了子进程myprog

2、SET-UID程序在普通用户态下运行：运行原有函数



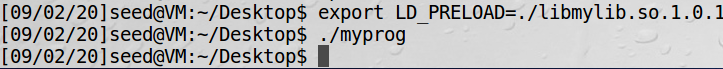
分析：动态链接库采取了防御措施，SET-UID的子进程不继承父进程的动态链接库的环境变量

3、SET-UID程序在root用户态下运行：运行自定义函数

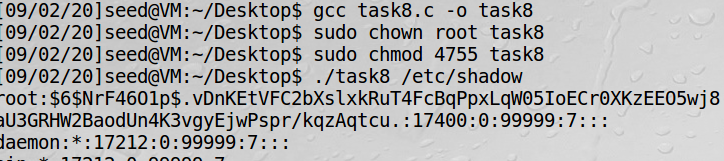


分析：root用户拥有shell执行特权，使得自定义环境变量得以传递

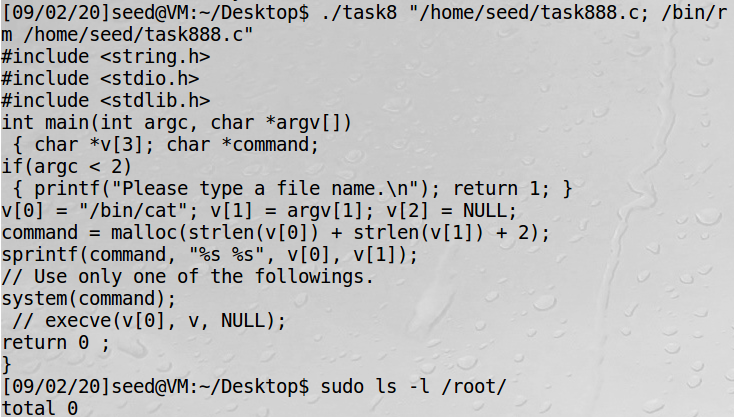
1. root用户状态下设置程序为setuid程序：  
   

Seed用户状态下修改环境变量，并运行程序：运行原有函数  


分析：两个用户间通过SET-UID程序，修改的环境变量不能被传递，起到了防御作用  
任务八：

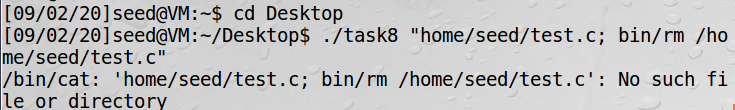
将程序变为特权程序：  


进入root状态并将.c文件拷贝到该目录下，运行:



通过sudo ls -l指令，发现目标文件被删除

注释掉system，换为execve：

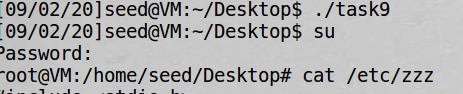


不可行：参数不可以被设置

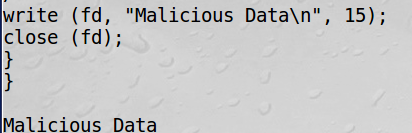
任务九：

创建特权文件：  


运行SET-UID程序：



特权文件被修改：



分析：最小特权原则：当SET-UID程序在不需要root特权时通过系统调用setuid()将其放弃。但是setuid只改变计算程序权限的用户，被修改后的权限可以通过保存的运行程序的用户的信息复原。