Lab1

57117221 姚远

TASK1

使用printenv命令查看环境变量

```
XDG_SEAT=seat0
LANGUAGE=en_US
GNOME DESKTOPSESSION_ID=this-is-deprecated
XDG_SESSION_DESKTOP=ubuntu
LOGNAME=seed
DBUS_SESSION_BUS_ADDRESS=unix:abstract=/tmp/dbus-uRCxZNvZIZ
J2SDKDIR=/usr/lib/jvm/java-8-oracle
XDG_DATA_DIRS=/usr/share/ubuntu:/usr/share/gnome:/usr/local/share/:/usr/sh
are/:/var/lib/snapd/desktop
QT4_IM_MODULE=xim
LESSOPEN=| /usr/bin/lesspipe %s
INSTANCE=
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
```

查看PWD的环境变量

```
[09/03/20]seed@VM:~$ printenv PWD
/home/seed
```

使用export命令设置环境变量

```
[09/03/20]seed@VM:~$ export YY=18
[09/03/20]seed@VM:~$ printenv YY
18
```

unset该变量，成功删除

```
[09/03/20]seed@VM:~$ unset YY
[09/03/20]seed@VM:~$ printenv YY
```

TASK2

编译手册中的代码，得到注释前的执行文件a.out与注释后的执行文件a1.out，以及两次得到的输出结果child与child1

对比两次输出，发现结果一致，证明子进程与父进程环境变量一致

TASK3

编译并执行t3，发现没有输出

```
[09/03/20]seed@VM:~/.../Task0$ gcc t3.c -o t3.out
t3.c: In function 'main':
t3.c:9:1: warning: implicit declaration of function 'execve' [-Wimplicit-function-declaration]
 execve("/usr/bin/env", argv, NULL);
 ^
[09/03/20]seed@VM:~/.../Task0$ ./t3.out
[09/03/20]seed@VM:~/.../Task0$ t3.out > t3
```

修改源代码之后，发现输出了系统的环境变量

```
GTK2_MODULES=overlay-scrollbar
SHLVL=1
HOME=/home/seed
XDG_SEAT=seat0
LANGUAGE=en_US
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
XDG_SESSION_DESKTOP=ubuntu
LOGNAME=seed
DBUS_SESSION_BUS_ADDRESS=unix:abstract=/tmp/dbus-jcYifTs2MG
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=
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
_=./t3.out
```

当环境变量并不在执行execve时被自动继承

TASK4

按照手册要求编译并执行

```
0;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
SHELL=/bin/bash
QT_ACCESSIBILITY=1
GDMSESSION=ubuntu
LESSCLOSE=/usr/bin/lesspipe %s %s
GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg- agent:0:1
UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1408
XDG_VTNR=7
QT_IM_MODULE=ibus
PWD=/home/seed/Desktop/Task0
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/sh
are/:/var/lib/snapd/desktop
VTE_VERSION=4205
JOB=dbus
```

TASK5

按照实验手册的要求编译程序，加入环境变量，运行发现并不是所有的环境变量都成功export，LD_LIBRARY_PATH没有成功export

```
[09/03/20]seed@VM:~/.../Task0$ export PATH='/usr'
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
[09/03/20]seed@VM:~/.../Task0$ export PATH='/bin
[09/03/20]seed@VM:~/.../Task0$ export LD_LIBRARY_PATH='/usr/bin'
[09/03/20]seed@VM:~/ .. ./Task0$ export YY=18
```

```
SHLVL=1
HOME=/home/seed
XDG_SEAT=seat0
LANGUAGE=en_US
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
XDG_SESSION_DESKTOP=ubuntu
```

```
LOGNAME=seed
DBUS_SESSION_BUSADDRESS=unix:abstract=/tmp/dbus-jcYifTs2MG
J2SDKDIR=/usr/lib/jvm/java-8-oracle
XDG_DATA_DIRS=/usr/share/ubuntu:/usr/share/gnome:/usr/local/share/:/usr/sh
are/:/var/lib/snapd/desktop
QT4_IM_MODULE=xim
LESSOPEN=/usr/bin/lesspipe %s
INSTANCE=
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
YY=18
XAUTHORITY=/home/seed/.Xauthority
 =./t5.out
```

TASK6

将_home_seed路径添加到PATH变量的最前面，并在_home_seed中加入自己替换的ls，即可得到输出“This is my ls”

```
[09/03/20]seed@VM:~/.../Task0$ export PATH=/home/seed:$PATH
[09/03/20]seed@VM:~/.../Task0$ ./ls
This is my ls
```

TASK7

不进行任何修改运行myprog

```
[09/03/20]seed@VM:~/.../Task0$ ./myprog
I am not sleeping!
```

将它修改为root用户的Set-UID程序，用普通用户权限运行

```
[09/03/20]seed@VM:~/.../Task0$ sudo chown root myprog
[09/03/20]seed@VM:~/.../Task0$ sudo chmod 4755 myprog
[09/03/20]seed@VM:~/.../Task0$ ./myprog
```

在root用户下export LD_PRELOAD，并运行

```
[09/03/20]seed@VM:~/.../Task0$ su
Password:
```

```
root@VM:/home/seed/Desktop/Task0# export LD_PREL0AD=./libmylib.so.1.0.1
root@VM:/home/seed/Desktop/Task0# ./myprog
I am not sleeping!
```

将myprog设定为user1的程序，在seed中exportLD_PRELOAD环境变量并运行

```
[09/03/20]seed@VM:~/.../Task0$ export LD_PREL0AD=./libmylib.so.1.0.1
[09/03/20]seed@VM:~/.../Task0$ ./myprog
```

系统内建的某种保护机制对LD_PRELOAD环境变量进行了保护

TASK8

创建一个名为secret的文件，并将其权限改为644 在向文件注入时，我们使用;rm -f 命令，删除系统中seed用户组只有只读权限的文件

```
[09/03/20]seed@VM:~/.../Task0$ ./t8 t5;rm -f secret
123
```

而将system改为execve后，发现删除失败，没有权限

```
[09/03/20]seed@VM:~/.../Task0$ ./t8 t5;rm -f /usr/secret
123
rm: cannot remove '/usr/secret': Rermission denied
```

TASK9

将源代码编译并执行，可以看到zzz中被加入了Malicious Data ， 说明普通用户得到了root权限

```
[09/03/20]seed@VM:~/.../Task0$ sudo chown root t9
[09/03/20]seed@VM:~/.../Task0$ sudo chmod 4755 t9
[09/03/20]seed@VM:~/.../Task0$ ./t9
```