

Lab1 Set-UID

许朝阳 57117212

Task 1: Manipulating Environment Variables

```
1. Script started on Wed 02 Sep 2020 11:25:21 AM EDT
2. [09/02/20]seed@VM:~/.../exp0$ printenv
3. XDG_VTNR=7
4. ORBIT_SOCKETDIR=/tmp/orbit-seed
5. XDG_SESSION_ID=c1
6. CLUTTER_IM_MODULE=xim
7. IBUS_DISABLE_SNOOPER=1
8. TERMINATOR_UUID=urn:uuid:95c7c41c-cc0d-429f-bcb1-6ff6a5011622
9. XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed
10. GIO_LAUNCHED_DESKTOP_FILE_PID=5498
11. SESSION=ubuntu
12. GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1
13. ANDROID_HOME=/home/seed/android/android-sdk-linux
14. SHELL=/bin/bash
15. TERM=xterm
16. DERBY_HOME=/usr/lib/jvm/java-8-oracle/db
17. QT_LINUX_ACCESSIBILITY_ALWAYS_ON=1
18. 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
19. WINDOWID=54525956
20. GNOME_KEYRING_CONTROL=
21. UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1723
22. GTK_MODULES=gail:atk-bridge:unity-gtk-module
23. USER=seed
24. LD_LIBRARY_PATH=/home/seed/source/boost_1_64_0/stage/lib:/home/seed/source/boost_1_64_0/stage/lib:
25. QT_ACCESSIBILITY=1
26. 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:

27. XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0

28. XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0

29. SSH_AUTH_SOCK=/run/user/1000/keyring/ssh

30. DEFAULTS_PATH=/usr/share/gconf/ubuntu.default.path

31. GIO_LAUNCHED_DESKTOP_FILE=/usr/share/applications/terminator.desktop

32. XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg

33. 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:/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

34. DESKTOP_SESSION=ubuntu

35. QT_QPA_PLATFORMTHEME=appmenu-qt5

36. QT_IM_MODULE=ibus

37. JOB=unity-settings-daemon

38. PWD=/home/seed/Documents/exp0

39. XDG_SESSION_TYPE=x11

40. JAVA_HOME=/usr/lib/jvm/java-8-oracle

41. XMODIFIERS=@im=ibus

42. LANG=en_US.UTF-8

43. GNOME_KEYRING_PID=

44. MANDATORY_PATH=/usr/share/gconf/ubuntu.mandatory.path

45. GDM_LANG=en_US

46. IM_CONFIG_PHASE=1

47. COMPIZ_CONFIG_PROFILE=ubuntu

48. GDMSESSION=ubuntu

49. GTK2_MODULES=overlay-scrollbar

50. SESSIONTYPE=gnome-session

51. XDG_SEAT=seat0

```
52. HOME=/home/seed
53. SHLVL=2
54. LANGUAGE=en_US
55. GNOME_DESKTOP_SESSION_ID=this-is-deprecated
56. UPSTART_INSTANCE=
57. LOGNAME=seed
58. UPSTART_EVENTS=xsession started
59. XDG_SESSION_DESKTOP=ubuntu
60. COMPIZ_BIN_PATH=/usr/bin/
61. QT4_IM_MODULE=xim
62. XDG_DATA_DIRS=/usr/share/ubuntu:/usr/share/gnome:/usr/local/share:/usr/share:/var/lib/snapd/desktop
63. J2SDKDIR=/usr/lib/jvm/java-8-oracle
64. DBUS_SESSION_BUS_ADDRESS=unix:abstract=/tmp/dbus-6fdnKSuHAI
65. LESSOPEN=| /usr/bin/lesspipe %s
66. UPSTART_JOB=unity7
67. INSTANCE=
68. DISPLAY=:0
69. XDG_RUNTIME_DIR=/run/user/1000
70. J2REDIR=/usr/lib/jvm/java-8-oracle/jre
71. GTK_IM_MODULE=ibus
72. XDG_CURRENT_DESKTOP=Unity
73. LESSCLOSE=/usr/bin/lesspipe %s %s
74. COLORTERM=gnome-terminal
75. XAUTHORITY=/home/seed/.Xauthority
76. _=/usr/bin/printenv
77. [09/02/20]seed@VM:~/.../exp0$ env
78. XDG_VTNR=7
79. ORBIT_SOCKETDIR=/tmp/orbit-seed
80. XDG_SESSION_ID=c1
81. CLUTTER_IM_MODULE=xim
82. IBUS_DISABLE_SNOOPER=1
83. TERMINATOR_UUID=urn:uuid:95c7c41c-cc0d-429f-bcb1-6ff6a5011622
84. XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed
85. GIO_LAUNCHED_DESKTOP_FILE_PID=5498
86. SESSION=ubuntu
87. GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1
88. ANDROID_HOME=/home/seed/android/android-sdk-linux
89. SHELL=/bin/bash
90. TERM=xterm
91. DERBY_HOME=/usr/lib/jvm/java-8-oracle/db
92. QT_LINUX_ACCESSIBILITY_ALWAYS_ON=1
```

93. 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

94. WINDOWID=54525956

95. GNOME_KEYRING_CONTROL=

96. UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1723

97. GTK_MODULES=gail:atk-bridge:unity-gtk-module

98. USER=seed

99. LD_LIBRARY_PATH=/home/seed/source/boost_1_64_0/stage/lib:/home/seed/source/boost_1_64_0/stage/lib:

100. QT_ACCESSIBILITY=1

101. 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:

102. XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0

103. XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0

104. SSH_AUTH_SOCK=/run/user/1000/keyring/ssh

105. DEFAULTS_PATH=/usr/share/gconf/ubuntu.default.path

106. GIO_LAUNCHED_DESKTOP_FILE=/usr/share/applications/terminator.desktop

107. XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg

108. 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:/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  
109. DESKTOP_SESSION=ubuntu  
110. QT_QPA_PLATFORMTHEME=appmenu-qt5  
111. QT_IM_MODULE=ibus  
112. JOB=unity-settings-daemon  
113. PWD=/home/seed/Documents/exp0  
114. XDG_SESSION_TYPE=x11  
115. JAVA_HOME=/usr/lib/jvm/java-8-oracle  
116. XMODIFIERS=@im=ibus  
117. LANG=en_US.UTF-8  
118. GNOME_KEYRING_PID=  
119. MANDATORY_PATH=/usr/share/gconf/ubuntu.mandatory.path  
120. GDM_LANG=en_US  
121. IM_CONFIG_PHASE=1  
122. COMPIZ_CONFIG_PROFILE=ubuntu  
123. GDMSESSION=ubuntu  
124. GTK2_MODULES=overlay-scrollbar  
125. SESSIONTYPE=gnome-session  
126. XDG_SEAT=seat0  
127. HOME=/home/seed  
128. SHLVL=2  
129. LANGUAGE=en_US  
130. GNOME_DESKTOP_SESSION_ID=this-is-deprecated  
131. UPSTART_INSTANCE=  
132. LOGNAME=seed  
133. UPSTART_EVENTS=xsession started  
134. XDG_SESSION_DESKTOP=ubuntu  
135. COMPIZ_BIN_PATH=/usr/bin/  
136. QT4_IM_MODULE=xim  
137. XDG_DATA_DIRS=/usr/share/ubuntu:/usr/share/gnome:/usr/local/share:/usr/sha  
re:/var/lib/snapd/desktop  
138. J2SDKDIR=/usr/lib/jvm/java-8-oracle  
139. DBUS_SESSION_BUS_ADDRESS=unix:abstract=/tmp/dbus-6fdnKSuHAI  
140. LESSOPEN=| /usr/bin/lesspipe %s  
141. UPSTART_JOB=unity7  
142. INSTANCE=  
143. DISPLAY=:0  
144. XDG_RUNTIME_DIR=/run/user/1000  
145. J2REDIR=/usr/lib/jvm/java-8-oracle/jre  
146. GTK_IM_MODULE=ibus  
147. XDG_CURRENT_DESKTOP=Unity  
148. LESSCLOSE=/usr/bin/lesspipe %s %s  
149. COLORTERM=gnome-terminal
```

```

150. XAUTHORITY=/home/seed/.Xauthority
151. _=/usr/bin/env
152. [09/02/20]seed@VM:~/.../exp0$ printenv PWS[KD
153. /home/seed/Documents/exp0
154. [09/02/20]seed@VM:~/.../exp0$ env |grep[K[K[K[K grep PWD
155. [01;31m[KPWD[m[K=/home/seed/Documents/exp0
156. [09/02/20]seed@VM:~/.../exp0$ printenv[K[K[K[K[K[K[K[Kexport Jason=112358
157. [09/02/20]seed@VM:~/.../exp0$ printenv[Kp[K[K[Kv Jason
158. 112358
159. [09/02/20]seed@VM:~/.../exp0$ env | grep Jason
160. [01;31m[KJason[m[K=112358
161. [09/02/20]seed@VM:~/.../exp0$ env | grep Jason[K[K[K[K[K[K112358
162. Jason=[01;31m[K112358[m[K
163. [09/02/20]seed@VM:~/.../exp0$ unsetenv[K Jason
164. [09/02/20]seed@VM:~/.../exp0$ printenv[Kenv Jason
165. [09/02/20]seed@VM:~/.../exp0$ env | grep Jason
166. [09/02/20]seed@VM:~/.../exp0$ env | grep Jason[K[K[K[K[K[K112358
167. [09/02/20]seed@VM:~/.../exp0$ exit
168. exit
169.
170. Script done on Wed 02 Sep 2020 11:29:24 AM EDT

```

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

Step 1:

首先阅读程序，了解到其目的为判断父进程子进程间环境变量是否又差异，于是依照手册指示，先将 step1.c 文件编译为 step1.o 文件，执行输出至 step1Out 文件。

Step 2:

将代码中①处注释，再取消②处注释，输出父进程的结果，重新编译得到 step2.o 文件，执行输出至 step2Out 文件。

Step 3:

使用 diff 指令判断 step1Out 与 step2Out 是否有差别，截图如下：

```

[09/02/20]seed@VM:~/.../code$ diff step1Out step2Out
74c74
< _=./step1.o
---
> _=./step2.o

```

发现二者的区别仅在于输入程序不同，其他相同，因此父进程与子进程间的环境变量并无差异。

Task 3: Environment Variables and execve()

Step 1:

了解 execve()函数

execve（执行文件）在父进程中fork一个子进程，在子进程中调用exec函数启动新的程序。exec函数一共有六个，其中execve为内核级系统调用，其他（execl，execl，execlp，execv，execvp）都是调用execve的库函数。

中文名	执行文件	父进程	fork
外文名	execve	作用	调用exec函数启动新的程序

目录	1 表头文件	3 函数说明	5 范例
	2 定义函数	4 返回值	6 执行

表头文件

```
#include<unistd.h>
```

定义函数

```
int execve(const char * filename,char * const argv[],char * const envp[ ]);
```

函数说明

execve()用来执行参数filename字符串所代表的文件路径，第二个参数是利用指针数组来传递给执行文件，并且需要以空指针(NULL)结束，最后一个参数则为传递给执行文件的新环境变量数组。

程序调用了 execve()函数，传入的 envp[]为空，程序执行后输出的环境变量为空。

Step 2:

将程序中①处改为：

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

子程序执行后输出的环境变量为输入的环境变量 environ。

Step 3:

当传入的 envp[]为 NULL 时，子程序的环境变量为空，当传入的 envp[]为 environ 即实际的环境变量时，子程序的环境变量为实际的环境变量，为验证，与 Task 2 中的输出结果进行比较，除文件路径不同外，其他均相同，截图如下：

```
[09/02/20]seed@VM:~/.../Task3$ diff prog20out ../Task2/step20out
36c36
< PWD=/home/seed/Documents/exp0/code/Task3
---
> PWD=/home/seed/Documents/exp0/code
74,75c74,75
< =./prog2.o
< OLDPWD=/home/seed/Documents/exp0/code
---
> =./step2.o
> OLDPWD=/home/seed/Documents/exp0
[09/02/20]seed@VM:~/.../Task3$ diff prog20out ../Task2/step10out
36c36
< PWD=/home/seed/Documents/exp0/code/Task3
---
> PWD=/home/seed/Documents/exp0/code
74,75c74,75
< =./prog2.o
< OLDPWD=/home/seed/Documents/exp0/code
---
> =./step1.o
> OLDPWD=/home/seed/Documents/exp0
```

Task 4: Environment Variables and system()

Step 1:

Linux/Unix函数

函数详解

(执行shell 命令)

相关函数

fork, execve, waitpid, popen

头文件

```
#include<stdlib.h>
```

定义函数

```
int system(const char * string);
```

函数说明

`system()` 会调用`fork()`产生子进程，由子进程来调用`/bin/sh -c string`来执行参数`string`字符串所代表的命令，此命令执行完后随即返回原调用的进程。在调用`system()`期间`SIGCHLD`信号会被暂时搁置，`SIGINT`和`SIGQUIT`信号则会被忽略。

返回值

如果fork（）失败 返回-1：出现错误

如果exec()失败，表示不能执行Shell，返回值相当于Shell执行了exit(127)

如果执行成功则返回子Shell的终止状态

了解 `system()` 函数，他与 `execve()` 函数的区别为：

execve() = command

```
system() = /bin/sh -c command
```

与exec的区别

- 1、system（）和exec（）都可以执行业务命令，system是在原进程上开辟了一个新的进程，但是exec是用新进程（命令）覆盖了原有的进程
- 2、system（）和exec（）都有能产生返回值，system的返回值并不影响原有进程，但是exec的返回值影响了原进程

运行程序得到 env 结果:

```

root@kali: ~# cat /etc/passwd | grep -v ^$ | sed -e 's/:/ /' | awk '{print $1, $2, $3, $4, $5, $6, $7, $8, $9, $10, $11, $12, $13, $14, $15, $16, $17, $18, $19, $20, $21, $22, $23, $24, $25, $26, $27, $28, $29, $30, $31, $32, $33, $34, $35, $36, $37, $38, $39, $40, $41, $42, $43, $44, $45, $46, $47, $48, $49, $50, $51, $52, $53, $54, $55, $56, $57, $58, $59, $60, $61, $62, $63, $64, $65, $66, $67, $68, $69, $70, $71, $72, $73, $74, $75, $76, $77, $78, $79, $80, $81, $82, $83, $84, $85, $86, $87, $88, $89, $90, $91, $92, $93, $94, $95, $96, $97, $98, $99, $100, $101, $102, $103, $104, $105, $106, $107, $108, $109, $110, $111, $112, $113, $114, $115, $116, $117, $118, $119, $120, $121, $122, $123, $124, $125, $126, $127, $128, $129, $130, $131, $132, $133, $134, $135, $136, $137, $138, $139, $140, $141, $142, $143, $144, $145, $146, $147, $148, $149, $150, $151, $152, $153, $154, $155, $156, $157, $158, $159, $160, $161, $162, $163, $164, $165, $166, $167, $168, $169, $170, $171, $172, $173, $174, $175, $176, $177, $178, $179, $180, $181, $182, $183, $184, $185, $186, $187, $188, $189, $190, $191, $192, $193, $194, $195, $196, $197, $198, $199, $200, $201, $202, $203, $204, $205, $206, $207, $208, $209, $210, $211, $212, $213, $214, $215, $216, $217, $218, $219, $220, $221, $222, $223, $224, $225, $226, $227, $228, $229, $230, $231, $232, $233, $234, $235, $236, $237, $238, $239, $240, $241, $242, $243, $244, $245, $246, $247, $248, $249, $250, $251, $252, $253, $254, $255, $256, $257, $258, $259, $260, $261, $262, $263, $264, $265, $266, $267, $268, $269, $270, $271, $272, $273, $274, $275, $276, $277, $278, $279, $280, $281, $282, $283, $284, $285, $286, $287, $288, $289, $290, $291, $292, $293, $294, $295, $296, $297, $298, $299, $300, $301, $302, $303, $304, $305, $306, $307, $308, $309, $310, $311, $312, $313, $314, $315, $316, $317, $318, $319, $320, $321, $322, $323, $324, $325, $326, $327, $328, $329, $330, $331, $332, $333, $334, $335, $336, $337, $338, $339, $340, $341, $342, $343, $344, $345, $346, $347, $348, $349, $350, $351, $352, $353, $354, $355, $356, $357, $358, $359, $360, $361, $362, $363, $364, $365, $366, $367, $368, $369, $370, $371, $372, $373, $374, $375, $376, $377, $378, $379, $380, $381, $382, $383, $384, $385, $386, $387, $388, $389, $390, $391, $392, $393, $394, $395, $396, $397, $398, $399, $400, $401, $402, $403, $404, $405, $406, $407, $408, $409, $410, $411, $412, $413, $414, $415, $416, $417, $418, $419, $420, $421, $422, $423, $424, $425, $426, $427, $428, $429, $430, $431, $432, $433, $434, $435, $436, $437, $438, $439, $440, $441, $442, $443, $444, $445, $446, $447, $448, $449, $450, $451, $452, $453, $454, $455, $456, $457, $458, $459, $460, $461, $462, $463, $464, $465, $466, $467, $468, $469, $470, $471, $472, $473, $474, $475, $476, $477, $478, $479, $480, $481, $482, $483, $484, $485, $486, $487, $488, $489, $490, $491, $492, $493, $494, $495, $496, $497, $498, $499, $500, $501, $502, $503, $504, $505, $506, $507, $508, $509, $510, $511, $512, $513, $514, $515, $516, $517, $518, $519, $520, $521, $522, $523, $524, $525, $526, $527, $528, $529, $530, $531, $532, $533, $534, $535, $536, $537, $538, $539, $540, $541, $542, $543, $544, $545, $546, $547, $548, $549, $550, $551, $552, $553, $554, $555, $556, $557, $558, $559, $560, $561, $562, $563, $564, $565, $566, $567, $568, $569, $570, $571, $572, $573, $574, $575, $576, $577, $578, $579, $580, $581, $582, $583, $584, $585, $586, $587, $588, $589, $590, $591, $592, $593, $594, $595, $596, $597, $598, $599, $600, $601, $602, $603, $604, $605, $606, $607, $608, $609, $610, $611, $612, $613, $614, $615, $616, $617, $618, $619, $620, $621, $622, $623, $624, $625, $626, $627, $628, $629, $630, $631, $632, $633, $634, $635, $636, $637, $638, $639, $640, $641, $642, $643, $644, $645, $646, $647, $648, $649, $650, $651, $652, $653, $654, $655, $656, $657, $658, $659, $660, $661, $662, $663, $664, $665, $666, $667, $668, $669, $670, $671, $672, $673, $674, $675, $676, $677, $678, $679, $680, $681, $682, $683, $684, $685, $686, $687, $688, $689, $690, $691, $692, $693, $694, $695, $696, $697, $698, $699, $700, $701, $702, $703, $704, $705, $706, $707, $708, $709, $710, $711, $712, $713, $714, $715, $716, $717, $718, $719, $720, $721, $722, $723, $724, $725, $726, $727, $728, $729, $730, $731, $732, $733, $734, $735, $736, $737, $738, $739, $740, $741, $742, $743, $744, $745, $746, $747, $748, $749, $750, $751, $752, $753, $754, $755, $756, $757, $758, $759, $760, $761, $762, $763, $764, $765, $766, $767, $768, $769, $770, $771, $772, $773, $774, $775, $776, $777, $778, $779, $780, $781, $782, $783, $784, $785, $786, $787, $788, $789, $790, $791, $792, $793, $794, $795, $796, $797, $798, $799, $800, $801, $802, $803, $804, $805, $806, $807, $808, $809, $810, $811, $812, $813, $814, $815, $816, $817, $818, $819, $820, $821, $822, $823, $824, $825, $826, $827, $828, $8
```


Task 5: Environment Variable and Set-UID Programs

Step 1:

阅读程序，其功能是循环输出所有环境变量。

Step 2:

将程序编译后更改所有者为 root，并将其设置为一个 Set-UID 程序，如下图：

[illegible]

Step 3:

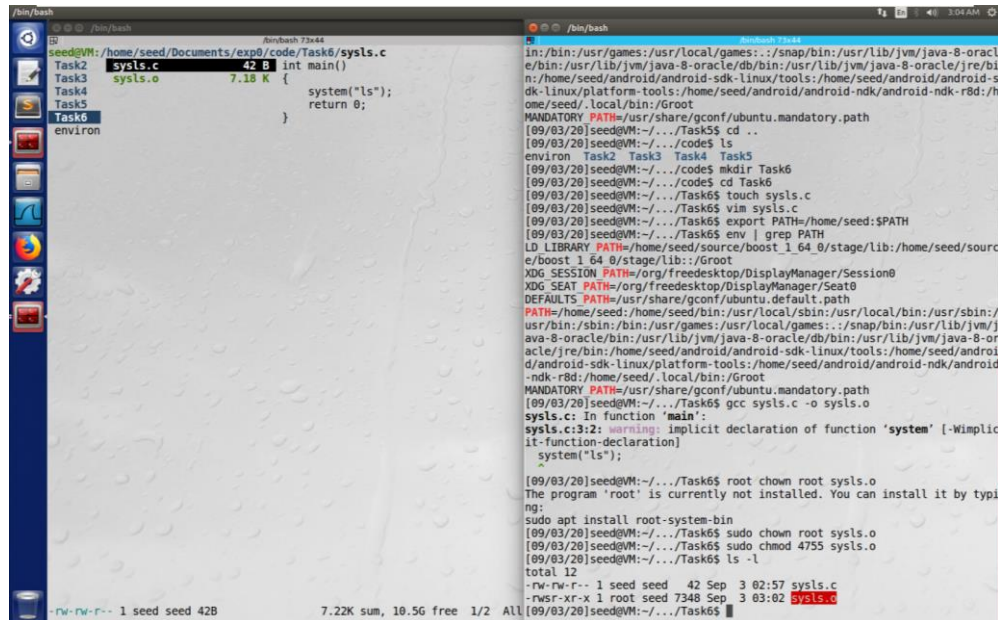
使用 export 指令对下列环境变量进行修改、创建，并运行 Set-UID 程序，发现在环境变量中存在新改动的环境变量，如下图：

[illegible]

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

Step 1:

使用 `export PATH=/home/seed:$PATH` 将路径添加至 PATH 前，编译程序后将目标文件权限修改为 root 所有，Set-UID 程序：

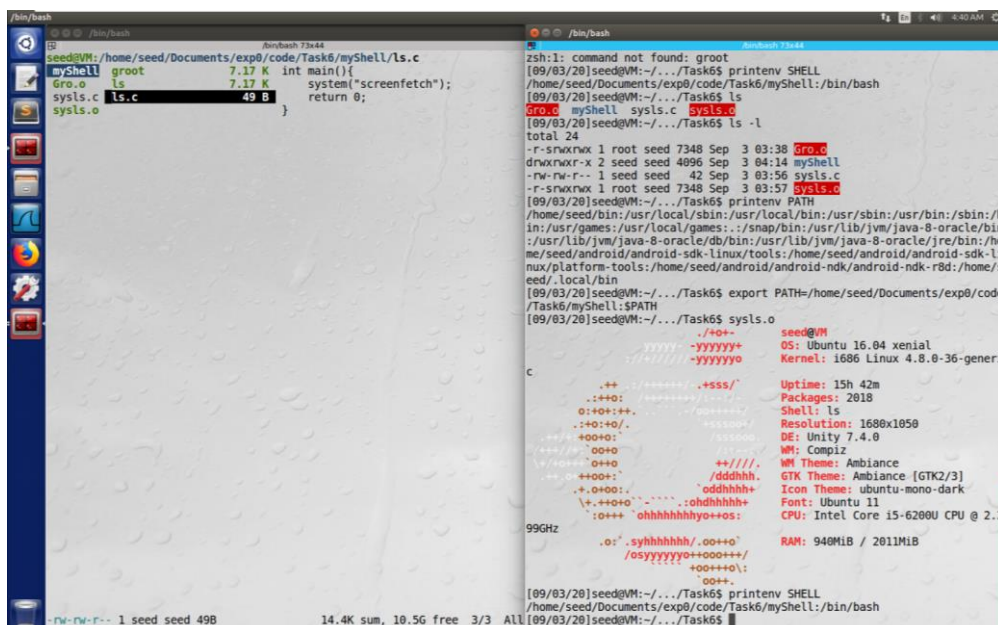


```
seed@VM: /home/seed/Documents/exp0/code/Task6/sysls.c
Task2 sysls.o 42 B
Task3 sysls.o 7.18 K
Task4
Task5
Task6
environ
int main()
{
    system("ls");
    return 0;
}

[09/03/20]seed@VM:~/.../Task6$ cd ..
[09/03/20]seed@VM:~/.../code$ ls
environ Task2 Task3 Task4 Task5
[09/03/20]seed@VM:~/.../code$ mkdir Task6
[09/03/20]seed@VM:~/.../code$ cd Task6
[09/03/20]seed@VM:~/.../Task6$ touch sysls.c
[09/03/20]seed@VM:~/.../Task6$ vim sysls.c
[09/03/20]seed@VM:~/.../Task6$ export PATH=/home/seed:$PATH
[09/03/20]seed@VM:~/.../Task6$ env | grep PATH
LD_LIBRARY_PATH=/home/seed/source/boost_1_64_0/stage/lib:/home/seed/source/boost_1_64_0/stage/lib:/Groot
XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0
XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0
DEFAULTS_PATH=/usr/share/gconf/ubuntu.default.path
PATH=/home/seed:/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:/Groot
MANDATORY_PATH=/usr/share/gconf/ubuntu.mandatory.path
[09/03/20]seed@VM:~/.../Task6$ gcc sysls.c -o sysls.o
[09/03/20]seed@VM:~/.../Task6$ root chown root sysls.o
The program 'root' is currently not installed. You can install it by typing:
sudo apt install root-system-bin
[09/03/20]seed@VM:~/.../Task6$ sudo chown root sysls.o
[09/03/20]seed@VM:~/.../Task6$ sudo chmod 4755 sysls.o
[09/03/20]seed@VM:~/.../Task6$ ls -l
total 12
-rw-rw-r-- 1 seed seed 42 Sep 3 02:57 sysls.c
-rwsr-xr-x 1 root seed 7348 Sep 3 03:02 sysls.o
[09/03/20]seed@VM:~/.../Task6$ sysls.o
sysls.c:3:2: warning: implicit declaration of function 'system' [-Wimplicit-function-declaration]
    system("ls");
    ^
[09/03/20]seed@VM:~/.../Task6$ root chown root sysls.o
The program 'root' is currently not installed. You can install it by typing:
sudo apt install root-system-bin
[09/03/20]seed@VM:~/.../Task6$ sudo chown root sysls.o
[09/03/20]seed@VM:~/.../Task6$ sudo chmod 4755 sysls.o
[09/03/20]seed@VM:~/.../Task6$ ls -l
total 12
-rw-rw-r-- 1 seed seed 42 Sep 3 02:57 sysls.c
-rwsr-xr-x 1 root seed 7348 Sep 3 03:02 sysls.o
[09/03/20]seed@VM:~/.../Task6$ sysls.o
sysls.c:3:2: warning: implicit declaration of function 'system' [-Wimplicit-function-declaration]
    system("ls");
    ^
```

Step 2:

将改写的 ls 函数修改为 screenfetch 指令，并编译为 ls 文件，运行 sysls.o 后得到被修改后的 ls 指令的结果，显示系统信息，如下图：



```
seed@VM: /home/seed/Documents/exp0/code/Task6/myShell/ls.c
myShell root 7.17 K int main()
{
    system("screenfetch");
    return 0;
}
Gro.o ls 7.17 K
sysls.c ls.c 49 B
sysls.o

[09/03/20]seed@VM:~/.../Task6$ gcc sysls.c -o sysls.o
[09/03/20]seed@VM:~/.../Task6$ root chown root sysls.o
The program 'root' is currently not installed. You can install it by typing:
sudo apt install root-system-bin
[09/03/20]seed@VM:~/.../Task6$ sudo chown root sysls.o
[09/03/20]seed@VM:~/.../Task6$ sudo chmod 4755 sysls.o
[09/03/20]seed@VM:~/.../Task6$ ls -l
total 24
-rwxrwxr-x 1 root seed 7348 Sep 3 03:38 Gro.o
drwxrwxr-x 2 seed seed 4096 Sep 3 04:14 myShell
-rw-rw-r-- 1 seed seed 42 Sep 3 03:56 sysls.c
-rwxrwxr-x 1 root seed 7348 Sep 3 03:57 sysls.o
[09/03/20]seed@VM:~/.../Task6$ printenv 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:/Groot
[09/03/20]seed@VM:~/.../Task6$ export PATH=/home/seed/Documents/exp0/code/Task6/myShell:$PATH
[09/03/20]seed@VM:~/.../Task6$ sysls.o
seed@VM
OS: Ubuntu 16.04 xenial
Kernel: i686 Linux 4.8.0-36-generic
Uptime: 15h 42m
Packages: 2018
Shell: ls
Resolution: 1680x1050
DE: Unity 7.4.0
WM: Compiz
VM Theme: Ambiance
GTK Theme: Ambiance [GTK2/3]
Icon Theme: ubuntu-mono-dark
Font: Ubuntu 11
CPU: Intel Core i5-6200U CPU @ 2.3
99GHz
RAM: 940MiB / 2011MiB
[09/03/20]seed@VM:~/.../Task6$ printenv SHELL
/home/seed/Documents/exp0/code/Task6/myShell:/bin/bash
[09/03/20]seed@VM:~/.../Task6$
```

Hint:

利用指令避开防御 Set-UID 被不安全利用的措施：

```
$ sudo rm /bin/sh
```

```
$ sudo ln -s /bin/zsh /bin/sh
```


Task 7: The LD PRELOAD Environment Variable and Set-UID Programs

Step 1:

准备工作，对程序进行编译，共享为动态链接库等操作。

Step 2:

在不同情况下运行程序观察不同用户的环境变量对其的影响，如下图组：

```
[09/03/20]seed@VM:~/.../Task7$ myprog.o
I am not sleeping!
```

regular program + normal user

```
[09/03/20]seed@VM:~/.../Task7$ sudo chown root myprog.o
[09/03/20]seed@VM:~/.../Task7$ sudo chmod 4577 myprog.o
[09/03/20]seed@VM:~/.../Task7$ ls -l
total 28
-rw-rw-r-- 1 seed seed  52 Sep  3 05:01 myprog.c
-r-srwxrwx 1 root seed 7348 Sep  3 05:01 myprog.o
-rw-rw-r-- 1 seed seed  151 Sep  3 04:57 sleep.c
-rw-rw-r-- 1 seed seed 2600 Sep  3 04:58 sleep.o
-rwxrwxr-x 1 seed seed 7940 Sep  3 04:59 sleep.so.1.0.1
[09/03/20]seed@VM:~/.../Task7$ myprog.o
[09/03/20]seed@VM:~/.../Task7$
```

Set-UID root program + normal user

```
[09/03/20]seed@VM:~/.../Task7$ su
Password:
root@VM:/home/seed/Documents/exp0/code/Task7# export LD_PRELOAD=./sleep.s
o.1.0.1
root@VM:/home/seed/Documents/exp0/code/Task7# printenv LD_PRELOAD
./sleep.so.1.0.1
root@VM:/home/seed/Documents/exp0/code/Task7# su seed
[09/03/20]seed@VM:~/.../Task7$ myprog.o
[09/03/20]seed@VM:~/.../Task7$ su
Password:
root@VM:/home/seed/Documents/exp0/code/Task7# myprog.o
root@VM:/home/seed/Documents/exp0/code/Task7# printenv LD_PRELOAD
/home/seed/lib/boost/libboost_program_options.so.1.64.0:/home/seed/lib/bo
ost/libboost_filesystem.so.1.64.0:/home/seed/lib/boost/libboost_system.so
.1.64.0
root@VM:/home/seed/Documents/exp0/code/Task7# export LD_PRELOAD=./sleep.s
o.1.0.1
root@VM:/home/seed/Documents/exp0/code/Task7# printenv LD_PRELOAD
./sleep.so.1.0.1
root@VM:/home/seed/Documents/exp0/code/Task7# myprog.o
I am not sleeping!
root@VM:/home/seed/Documents/exp0/code/Task7#
```

Set-UID root program + root user with new LD_PRELOAD

```
[09/03/20]seed@VM:~/.../Task7$ whoami
seed
[09/03/20]seed@VM:~/.../Task7$ sudo chown seed myprog.o
[09/03/20]seed@VM:~/.../Task7$ sudo chmod 4577 myprog.o
```

```

root@VM:/home/seed/Documents/exp0/code/Task7# useradd user2
root@VM:/home/seed/Documents/exp0/code/Task7# su user2
user2@VM:/home/seed/Documents/exp0/code/Task7$ whoami
user2
user2@VM:/home/seed/Documents/exp0/code/Task7$ printenv LD_PRELOAD
/home/seed/lib/boost/libboost_program_options.so.1.64.0:/home/seed/lib/bo
ost/libboost_filesystem.so.1.64.0:/home/seed/lib/boost/libboost_system.so
.1.64.0
user2@VM:/home/seed/Documents/exp0/code/Task7$ export LD_PRELOAD=./sleep.
so.1.0.1
user2@VM:/home/seed/Documents/exp0/code/Task7$ printenv LD_PRELOAD
./sleep.so.1.0.1
user2@VM:/home/seed/Documents/exp0/code/Task7$ ls -l
total 28
-rw-rw-r-- 1 seed seed 52 Sep 3 05:01 myprog.c
-r-srwxrwx 1 seed seed 7348 Sep 3 05:01 myprog.o
-rw-rw-r-- 1 seed seed 151 Sep 3 04:57 sleep.c
-rw-rw-r-- 1 seed seed 2600 Sep 3 04:58 sleep.o
-rwxrwxr-x 1 seed seed 7940 Sep 3 04:59 sleep.so.1.0.1
user2@VM:/home/seed/Documents/exp0/code/Task7$ myprog.o
user2@VM:/home/seed/Documents/exp0/code/Task7$ ls

```

SET-UID user1 program + normal user2 with new LD_PRELOAD

Step 3:

从以上结果可总结，当程序的执行者拥有相应的环境变量时，才会依照对应的动态链接库运行，对于拥有者和 root 用户来说都相同，而对于 Set-UID 程序来说，需要 root 的环境变量有相应动态链接库才能对应地运行，补充进行实验观察到当 root 退出时相当于关闭 root 的 shell，因此环境变量会恢复为正常情况下的环境变量，之后进入 root 环境变量也是修改前的状态，因此当另一个普通用户以 root 身份运行 Set-UID 程序时，环境变量以 root 用户为准，在运行 Set-UID 程序时将普通用户的环境变量传给 root 用户，则普通用户会以 root 权限以普通用户传递给 root 用户的环境变量为准，加载对应的动态链接库并得到相应的实验结果。

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

Step 1:

将所给程序编译并设为 root 用户的 Set-UID 程序，观察函数语句可构造特别字符串使其执行多条指令，本次输入指令为：

```
sysBob.o ~/.vim/vimrc;mv ~/Documents/exp0/code/Task8/test ~/Documents/exp0/code/Task8/Groot
```

```
sysBob.o ~/.vim/vimrc;rm ~/Documents/exp0/code/Task8/Groot
```

分别执行重命名与删除文件的操作，以下操作证明对普通文件与高权限文件均成功：

```
Terminator
root@VM: /home/seed/Documents/exp0/code/Task7
map <LEADER><left> :vertical resize-5<CR>
map <LEADER><right> :vertical resize+5<CR>

map tu :tabe<CR>
map t- :tabnext<CR>
map t+ :+tabnext<CR>

map sv <C-W>t<C-W>H
map sh <C-W>t<C-W>K

map <LEADER>sc :set spell!<CR>
map tx :r !figlet

set nocompatible
filetype on
filetype indent on
filetype plugin on
filetype plugin indent on

set mouse=a
set encoding=utf-8

set scrolloff=8
set backspace=indent,eol,start
set foldmethod=indent
set foldlevel=99

au BufReadPost * if line("\n") > 1 && line("\n") <= line("$") | exe "normal! g'\n" | endif

let <SI> = "\<Esc>]50;CursorShape=1\x7"
let <SR> = "\<Esc>]50;CursorShape=2\x7"
let <EI> = "\<Esc>]50;CursorShape=0\x7"

" call plug#begin('~/.vim/plugged')
" Plug 'vim-airline/vim-airline'
" Plug 'ycm-core/YouCompleteMe'

" call plug#end()
[09/03/20]seed@VM:~/.../Task8$ sysBob.o ~/Documents/exp0/code/Task8/test;
mv ~/Documents/exp0/code/Task8/test ~/Documents/exp0/code/Task8/Groot]
```

```
Terminator
root@VM: /home/seed/Documents/exp0/code/Task7
map tu :tabe<CR>
map t- :tabnext<CR>
map t+ :+tabnext<CR>

map sv <C-W>t<C-W>H
map sh <C-W>t<C-W>K

map <LEADER>sc :set spell!<CR>
map tx :r !figlet

set nocompatible
filetype on
filetype indent on
filetype plugin on
filetype plugin indent on

set mouse=a
set encoding=utf-8

set scrolloff=8
set backspace=indent,eol,start
set foldmethod=indent
set foldlevel=99

au BufReadPost * if line("\n") > 1 && line("\n") <= line("$") | exe "normal! g'\n" | endif

let <SI> = "\<Esc>]50;CursorShape=1\x7"
let <SR> = "\<Esc>]50;CursorShape=2\x7"
let <EI> = "\<Esc>]50;CursorShape=0\x7"

" call plug#begin('~/.vim/plugged')
" Plug 'vim-airline/vim-airline'
" Plug 'ycm-core/YouCompleteMe'

" call plug#end()
[09/03/20]seed@VM:~/.../Task8$ sysBob.o ~/Documents/exp0/code/Task8/test;
mv ~/Documents/exp0/code/Task8/test ~/Documents/exp0/code/Task8/Groot
Will you miss me?
[09/03/20]seed@VM:~/.../Task8$ ]
```



```
/bin/bash
seed@VM: /home/seed/Documents/exp0/code/Task8/Groot
Task2 backup 18 B
Task3 Bob.c 433 B
Task4 Groot 18 B
Task5 sysBob.o 7.37 K
Task6
Task7
Task8
environ

--w----- 1 root seed 188 7.83K sum, 10.5G free 3/4 AU
```

```
root@VM: /home/seed/Documents/exp0/code/Task8
[09/03/20]seed@VM:~/.../Task8$ ls
Bob.c sysBob.o
[09/03/20]seed@VM:~/.../Task8$ touch Groot
[09/03/20]seed@VM:~/.../Task8$ vim Groot
[09/03/20]seed@VM:~/.../Task8$ sudo chown root Groot
[09/03/20]seed@VM:~/.../Task8$ ls -l
total 16
-rw-rw-r-- 1 seed seed 433 Sep 3 05:59 Bob.c
-rw-rw-r-- 1 root seed 18 Sep 3 11:40 Groot
-r-srwxrwx 1 root seed 7544 Sep 3 06:00 sysBob.o
[09/03/20]seed@VM:~/.../Task8$ rm Groot
[09/03/20]seed@VM:~/.../Task8$ vim Groot
[09/03/20]seed@VM:~/.../Task8$ touch Groot
[09/03/20]seed@VM:~/.../Task8$ sudo chmod 700 Groot
[09/03/20]seed@VM:~/.../Task8$ ls -l
total 16
-rw-rw-r-- 1 seed seed 433 Sep 3 05:59 Bob.c
-rw-rw-r-- 1 seed seed 18 Sep 3 11:41 Groot
-r-srwxrwx 1 root seed 7544 Sep 3 06:00 sysBob.o
[09/03/20]seed@VM:~/.../Task8$ rm Groot
[09/03/20]seed@VM:~/.../Task8$ vim Groot
[09/03/20]seed@VM:~/.../Task8$ cp Groot backup
[09/03/20]seed@VM:~/.../Task8$ su
Password:
root@VM:/home/seed/Documents/exp0/code/Task8# chown root Groot
root@VM:/home/seed/Documents/exp0/code/Task8# chmod 100 Groot
root@VM:/home/seed/Documents/exp0/code/Task8# ls -l
total 20
-rw-rw-r-- 1 seed seed 18 Sep 3 11:43 backup
-rw-rw-r-- 1 seed seed 433 Sep 3 05:59 Bob.c
--x----- 1 root seed 18 Sep 3 11:43 Groot
-r-srwxrwx 1 root seed 7544 Sep 3 06:00 sysBob.o
root@VM:/home/seed/Documents/exp0/code/Task8# chmod 200 Groot
root@VM:/home/seed/Documents/exp0/code/Task8# ls -l
total 20
-rw-rw-r-- 1 seed seed 18 Sep 3 11:43 backup
-rw-rw-r-- 1 seed seed 433 Sep 3 05:59 Bob.c
--w----- 1 root seed 18 Sep 3 11:43 Groot
-r-srwxrwx 1 root seed 7544 Sep 3 06:00 sysBob.o
root@VM:/home/seed/Documents/exp0/code/Task8# exit
exit
[09/03/20]seed@VM:~/.../Task8$ rm Groot
rm: remove write-protected regular file 'Groot'?
[09/03/20]seed@VM:~/.../Task8$
```

```
/bin/bash
seed@VM: /home/seed/Documents/exp0/code/Task8/sysBob.o
Task2 backup 18 B
Task3 Bob.c 433 B
Task4 sysBob.o 7.37 K
Task5
Task6
Task7
Task8
environ

-r-xrwxrwx 1 root seed 7.37K 7.81K sum, 10.5G free 3/3 AU
```

```
root@VM: /home/seed/Documents/exp0/code/Task8
[09/03/20]seed@VM:~/.../Task8$ rm Groot
[09/03/20]seed@VM:~/.../Task8$ touch Groot
[09/03/20]seed@VM:~/.../Task8$ vim Groot
[09/03/20]seed@VM:~/.../Task8$ sudo chmod 700 Groot
[09/03/20]seed@VM:~/.../Task8$ ls -l
total 16
-rw-rw-r-- 1 seed seed 433 Sep 3 05:59 Bob.c
-rw-rw-r-- 1 seed seed 18 Sep 3 11:41 Groot
-r-srwxrwx 1 root seed 7544 Sep 3 06:00 sysBob.o
[09/03/20]seed@VM:~/.../Task8$ rm Groot
[09/03/20]seed@VM:~/.../Task8$ vim Groot
[09/03/20]seed@VM:~/.../Task8$ cp Groot backup
[09/03/20]seed@VM:~/.../Task8$ su
Password:
root@VM:/home/seed/Documents/exp0/code/Task8# chown root Groot
root@VM:/home/seed/Documents/exp0/code/Task8# chmod 100 Groot
root@VM:/home/seed/Documents/exp0/code/Task8# ls -l
total 20
-rw-rw-r-- 1 seed seed 18 Sep 3 11:43 backup
-rw-rw-r-- 1 seed seed 433 Sep 3 05:59 Bob.c
--x----- 1 root seed 18 Sep 3 11:43 Groot
-r-srwxrwx 1 root seed 7544 Sep 3 06:00 sysBob.o
root@VM:/home/seed/Documents/exp0/code/Task8# chmod 200 Groot
root@VM:/home/seed/Documents/exp0/code/Task8# ls -l
total 20
-rw-rw-r-- 1 seed seed 18 Sep 3 11:43 backup
-rw-rw-r-- 1 seed seed 433 Sep 3 05:59 Bob.c
--w----- 1 root seed 18 Sep 3 11:43 Groot
-r-srwxrwx 1 root seed 7544 Sep 3 06:00 sysBob.o
root@VM:/home/seed/Documents/exp0/code/Task8# exit
exit
[09/03/20]seed@VM:~/.../Task8$ rm Groot
rm: remove write-protected regular file 'Groot'?
[09/03/20]seed@VM:~/.../Task8$ sysBob.o ~/Documents/exp0/code/Task8/Groot
;rm ~/Documents/exp0/code/Task8/Groot
Will you miss me?
[09/03/20]seed@VM:~/.../Task8$ sysBob.o ~/Documents/exp0/code/Task8/Groot
;rm ~/Documents/exp0/code/Task8/Groot
Will you miss me?
rm: remove write-protected regular file '/home/seed/Documents/exp0/code/T
ask8/Groot'? yes
[09/03/20]seed@VM:~/.../Task8$
```

Step 2:

当使用 `execve()` 而不是 `system()` 函数时, 攻击不成功, 因为 `execve()` 将名称看作文件名, 提示找不到此文件。

Task 9: Capability Leaking

Step 1:

首先将程序编译，改为 root 拥有，设置为 Set-UID 程序，创建/etc/zzz 文件，运行程序可发现敏感文件 zzz 文件已被恶意修改，原因是在文件打开的时候未降回权限，导致对敏感文件的读写权限还停留在 root，造成能力泄露的问题，攻击者乘虚而入。

