## 1.1 Linux 系统文件权限设置与辨识 setuid 程序 uid 差异（5 分）

1、 设计并实现不同用户对不同类文件的 r、w、x 权限:

（1）查看系统文件的权限设置

a)查看/etc/passwd 文件和/etc/bin/passwd 文件的权限设置，并分析其权限为什么这么设置;

```
ubuntu@ubuntu-VirtualBox:~$ ls -lth /etc/passwd
-rw-r--r-- 1 root root 2.8K Mar 16  2021 /etc/passwd
ubuntu@ubuntu-VirtualBox:~$ ls -lth /bin/passwd
-rwsr-xr-x 1 root root 67K May 28  2020 /bin/passwd
ubuntu@ubuntu-VirtualBox:~$
```

/etc/passwd 是一个基于纯文本的数据库，其中包含系统上所有用户帐户的信息。 它归 root 所有并拥有 644 权限。该文件只能由 root 或具有 sudo 权限的用 户修改，并且所有系统用户都可以读取。除非你知道自己在做什么，否则应避免手 动修改 /etc/passwd 文件。 始终使用专为此目的设计的命令。 例如，要修改用 户帐户，请使用 usermod 命令，并使用 useradd 命令添加新用户帐户。 /etc/passwd 文件跟踪系统上的所有用户。

/bin/passwd 用于修改用户密码，任何用户都可以调用。 该文件由 root 创建，密码存储在 /etc/shadow 文件中。 由于/etc/shadow 文件只允许 root 读写，所以/bin/passwd 设置密码必须以 root 身份执行。

b)找到 2 个设置了 setuid 位的可执行程序，该程序的功能，该程序如果不设置 setuid 位是否能够达到相应的功能，

```
ubuntu@ubuntu-VirtualBox:~$ ls -lth /bin/ping
-rwxr-xr-x 1 root root 75K Aug 24  2020 /bin/ping
ubuntu@ubuntu-VirtualBox:~$ ls -lth /bin/mount
-rwsr-xr-x 1 root root 55K Aug 31  2020 /bin/mount
ubuntu@ubuntu-VirtualBox:~$
```

ping 命令是一个简单的实用程序，用于检查网络是否可用以及主机是否可达。使用此命令，您可以测试服务器是否已启动并正在运行。mount 程序用于在空文件夹中 mount 分区或设备。这两个命令动作都需要 root 权限，普通用户无法执行，所以需要设置 setuid 位，使运行这两个程序的 euid 为 root。

（2）设置文件或目录权限

a)用户 A 具有文本文件”流星雨.txt”，该用户允许别人下载；

```
ubuntu@ubuntu-VirtualBox:~/Desktop$ sudo adduser testuser
Adding user `testuser' ...
Adding new group `testuser' (1002) ...
Adding new user `testuser' (1002) with group `testuser' ...
Creating home directory `/home/testuser' ...
Copying files from `/etc/skel' ...
New password:
BAD PASSWORD: The password contains the user name in some form
Retype new password:
passwd: password updated successfully
Changing the user information for testuser
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n]
ubuntu@ubuntu-VirtualBox:~/Desktop$ su --login testuser
Password:
testuser@ubuntu-VirtualBox:~$
```

```
testuser@ubuntu-VirtualBox:~$ pwd
/home/testuser
testuser@ubuntu-VirtualBox:~$ touch 流星雨.txt
testuser@ubuntu-VirtualBox:~$ ls -l
total 0
-rw-rw-r-- 1 testuser testuser 0 พ.ย.  28 00:28 流星雨.txt
```

首先创建用户 testuser，然后登入并 touch 该文件来测试。该用户允许别人下载，touch 文件之后权限位可设置为 664，当切换到其他用户，仍然可以读取该文件。

b)用户 A 编译了一个可执行文件”cal.exe”，该用户想在系统启动时运行；

```
testuser@ubuntu-VirtualBox:~$ vi cal.c
testuser@ubuntu-VirtualBox:~$ gcc cal.c -o cal.exe
testuser@ubuntu-VirtualBox:~$ ls -lth
total 24K
-rwxrwxr-x 1 testuser testuser 17K พ.ย.  28 00:40 cal.exe
-rw-rw-r-- 1 testuser testuser 127 พ.ย.  28 00:40 cal.c
-rw-rw-r-- 1 testuser testuser   0 พ.ย.  28 00:28 流星雨.txt
testuser@ubuntu-VirtualBox:~$
```

首先创建 c 文件并编译为 cal.exe，无法确认哪个用户启动，所以必须给所有用户可以执行该文件的执行权限。

c)用户 A 有起草了文件”demo.txt”，想让同组的用户帮其修改文件；

```
testuser@ubuntu-VirtualBox:~$ touch demo.txt
testuser@ubuntu-VirtualBox:~$ chmod g+w demo.txt
testuser@ubuntu-VirtualBox:~$ ls -lth demo.txt
-rw-rw-r-- 1 testuser testuser 0 ₩.₪.  28 01:00 demo.txt
testuser@ubuntu-VirtualBox:~$
```

将文件的权限设置 g+w 即可，同组的用户就拥有读写权限。

d)一个 root 用户拥有的网络服务程序”netmonitor.exe”，需要设置 setuid 位才能完成其功能。

```
testuser@ubuntu-VirtualBox:~$ chmod u+s netmonitor.exe
testuser@ubuntu-VirtualBox:~$ ls -lth
total 20K
-rwsrwxr-x 1 testuser testuser 17K ₩.₪.  28 00:40 netmonitor.exe
testuser@ubuntu-VirtualBox:~$
```

创建该文件之后，设置的权限 u+s 即可。

2、 一些可执行程序运行时需要系统管理员权限，在 UNIX 中可以利用 setuid 位实现其功能，但 setuid 了的程序运行过程中拥有了 root 权限，因此在完成管理操作后需要切换到普通用户的身份执行后续操作。

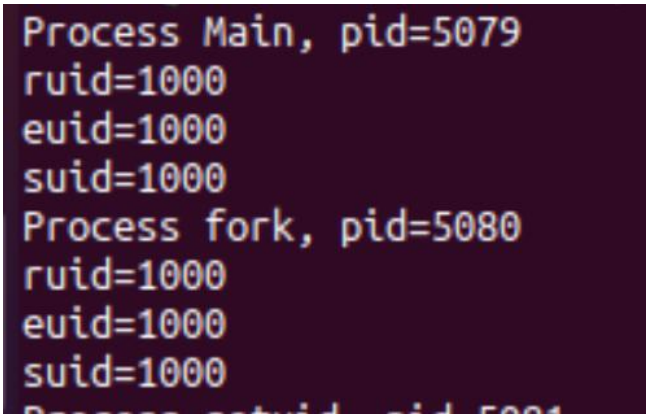
```
ubuntu@ubuntu-VirtualBox:~/Desktop/lab1$ ls -lth *.o
-rwxr-xr-x 1 ubuntu ubuntu 17K Nov 28 20:36 echo.o
-rws--x--x 1 ubuntu ubuntu 17K Nov 28 20:30 setuid.o
-rwx------ 1 ubuntu ubuntu 17K Nov 28 20:25 kill.o
-rwx------ 1 ubuntu ubuntu 17K Nov 28 19:39 http_server.o
ubuntu@ubuntu-VirtualBox:~/Desktop/lab1$
```

(1)设想一种场景，比如提供 http 网络服务，需要设置 setuid 位，并为该场景编制相应的代码；

```
ubuntu@ubuntu-VirtualBox:~/Desktop/lab1$ ./http_server.o
Process http, pid=5173
ruid=1000
euid=1000
suid=1000
```

euid，suid = ruid 就可以以 root 身份执行

(2)如果用户 fork 进程后，父进程和子进程中 euid、ruid、suid 的差别；




当 fork 的 child 进程中查看 ruid，suid，euid 和 parent 进程 Main 是相同。

(3)利用 execl 执行 setuid 程序后，euid、ruid、suid 是否有变化；

利用 execl 执行 setuid 程序后，euid、ruid、suid 不变，以 root 身份执行。

(4)程序何时需要临时性放弃 root 权限，何时需要永久性放弃 root 权限，并在程序中分别实现两种放弃权限方法；

临时放弃权限时，将 etreuid(ruid,euid,suid) 的 euid 保存在 suid，然后 euid 设置为当前的 ruid。

setreuid(ruid,euid,suid) 永久性放弃权限时，把 euid，suid 都设置为 ruid=1000。

(5)execl 函数族中有多个函数，比较有环境变量和无环境变量的函数使用的差异。

使用 execl 函数时，该函数会使用进程的环境变量作为新执行程序的环境变量。使用 exetle 函数时，需要传递一个指向环境变量字符串的指针来自定义新的执行程序的环境。 多变的。

3、 编制实验报告，对问题一说明原理，对问题 2 说明设计过程和实验步骤。并写出心得体会。

通过此题目更了解了 Linux 中的权限，Linux 使用位的组合来存储文件的权限。 我们可以使用更改权限，这实质上更改了与文件关联的“r”、“w”和“x”字符。

## 1.2 chroot 的配置

1、 利用 chroot 工具来虚拟化管理

1) 实现 bash 或 ps 的配置使用；

```
osboxes@osboxes:~$ whereis chroot
chroot: /usr/sbin/chroot /usr/share/man/man8/chroot.8.gz
osboxes@osboxes:~$ ldd /usr/sbin/chroot
        linux-vdso.so.1 (0x00007fff8adf0000)
        libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007f8f6dd8b0
        /lib64/ld-linux-x86-64.so.2 (0x00007f8f6df95000)
osboxes@osboxes:~$
```

创建命令运行的所有基本目录，创建所有这些目录以保留所需库的副本,复制适当的库/对象：为了让 Jaileddirectory 中的可执行文件工作，我们需要复制 JAILED 目录中的适当库/对象。 默认情况下，可执行文件查看以“/”开头的位置。 要查找依赖项，我们使用命令“ldd”。

2) 利用 chroot 实现 SSH 服务或 FTP 服务的虚拟化隔离；

```
ubuntu@ubuntu-VirtualBox:~$ sudo mkdir /home/ubuntu/{ftp_up,ftp_down}
ubuntu@ubuntu-VirtualBox:~$ sudo chmod 755 /home/ubuntu/{ftp_up,ftp_down}
ubuntu@ubuntu-VirtualBox:~$ sudo chown ubuntu:ubuntu /home/ubuntu/{ftp_up,ftp_down}
```

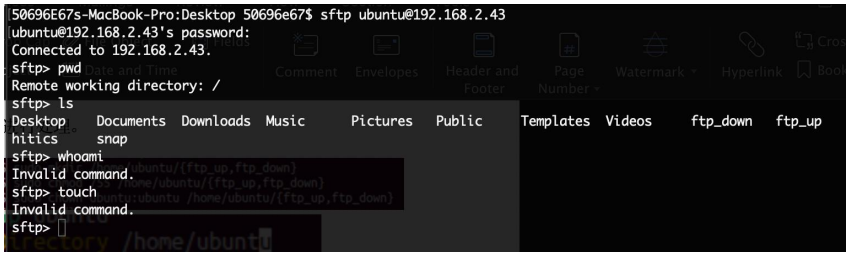
```
ChrootDirectory /home/ubuntu
```

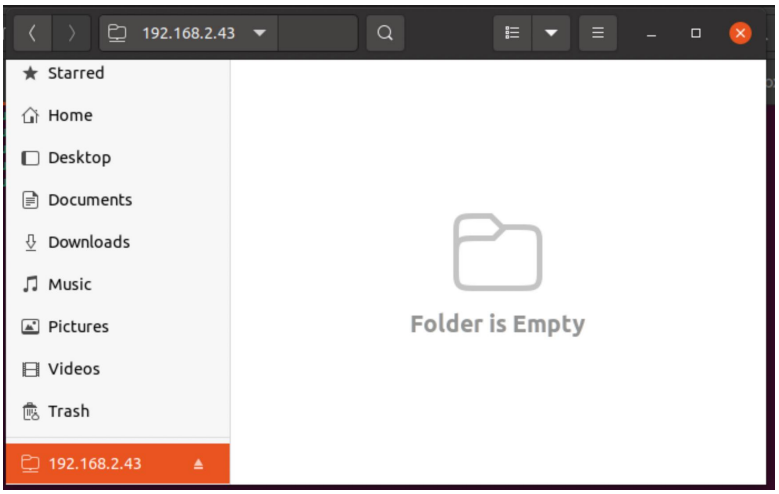
由于用户的目录现在归 root 所有，他们将无法创建文件和/或目录。 为了解决这个问题（以便他们可以上传和下载文件），创建新的子目录（在他们的主目录中），他们可以使用以下命令访问这些子目录。

现在我们需要配置 SSH。 发出命令：sudo vim /etc/ssh/sshd_config
在该文件中，查找以下行：子系统 sftp /usr/lib/openssh/sftp-server
将该行更改为：子系统 sftp internal-sftp
滚动到文件底部并添加以下内容：
仅匹配组
    Chrootdirecroty $HOME
    ForceCommand internal-sftp

AllowTcpForwarding no
X11Forwarding no

保存文件之后使用以下命令重新启动 SSH 守护进程。




成功通过身份验证后，发出命令 pwd 以检查当前工作目录。 它应该报告并且不允许该用户访问该目录之外的任何内容。

发出命令 ls 查看允许用户访问的新创建的目录，成功通过身份验证后，发出命令 pwd 以检查当前工作目录。 它应该报告并且不允许该用户访问该目录之外的任何内容。

3) chroot 后如何降低权限，利用实验一中编制的程序检查权限的合理性；

4)在 chroot 之前没有采用 cd xx 目录，会对系统有何影响，编制程序分析其影响。

最好编写一个脚本并在 chroot 中执行该脚本，而不是按命令执行命令。“cd”不是一个真正的命令，它是 sh/dash/bash/zsh/ksh 的内置命令，所以你必须启动 bash 并告诉它“cd”。

可参考后面的文件内容进行处理。

2、 编制实验报告，说明原理，设计过程和实验步骤。并写出心得体会。

通过本题目我已经了解更多，有一个 SFTP 设置，使用户只能访问特定目录。 确保锁定需要在该服务器上使用 SFTP 的每个用户，然后您就可以开始使用了。

中，所以在 pwd_mkdb 后面加上-d 参数来指定数据库存放位置：

#pwd_mkdb -d /var/chroot/etc /var/chroot/etc/master.passwd

此时如果执行成功的话将会在/var/chroot/etc/目录中多“pwd.db、spwd.db”两个文件。

**2.3 再次进入 chroot 环境：**

#chroot /var/chroot /usr/libexec/ftpd.sh

现在便可以登录到 chroot 环境下的 ftp 服务器了。

# 3、结尾工作

为每一个用户建立 home 目录，注意是在建在/var/chroot/home 之中。在/var/chroot/etc/中生成 ftpusers 文件，将禁止登录 ftp 的用户的用户名加入其中，以禁止部分用户登录。

在/var/chroot/etc/中生成 ftpchroot 文件，它的作用是限制用户只能访问自己的 home 目录中的文件，而不能访问 home 外的任何内容。将要限制的用户用户名加入其中。

在/var/chroot/etc/中生成 ftpwelcome 文件，它的作用是当用户连接上服务器的时候显示欢迎信息。在/var/chroot/etc/中生成 ftpmotd 文件，它的作用是当用户登录进服务器的时候显示欢迎信息。