



兄弟连教育

[www.lampbrother.net](http://www.lampbrother.net)

# 第八讲 权限管理

主讲人：沈超（<http://weibo.com/lampsc>）

交流论坛：<http://bbs.lampbrother.net>

无兄弟 不编程！

# 课程大纲

8.1 ACL权限

8.2 文件特殊权限

8.3 文件系统属性chattr权限

8.4 系统命令sudo权限

## 8.2 文件特殊权限

### 8.2.1 SetUID

### 8.2.2 SetGID

### 8.3.3 Sticky BIT

# 1、SetUID的功能

- ◆ 只有可以执行的二进制程序才能设定SUID权限
- ◆ 命令执行者要对该程序拥有x（执行）权限
- ◆ 命令执行者在执行该程序时获得该程序文件属主的身份（在执行程序的过程中灵魂附体为文件的属主）
- ◆ SetUID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

- ◆ passwd命令拥有SetUID权限，所以普通用户可以修改自己的密码

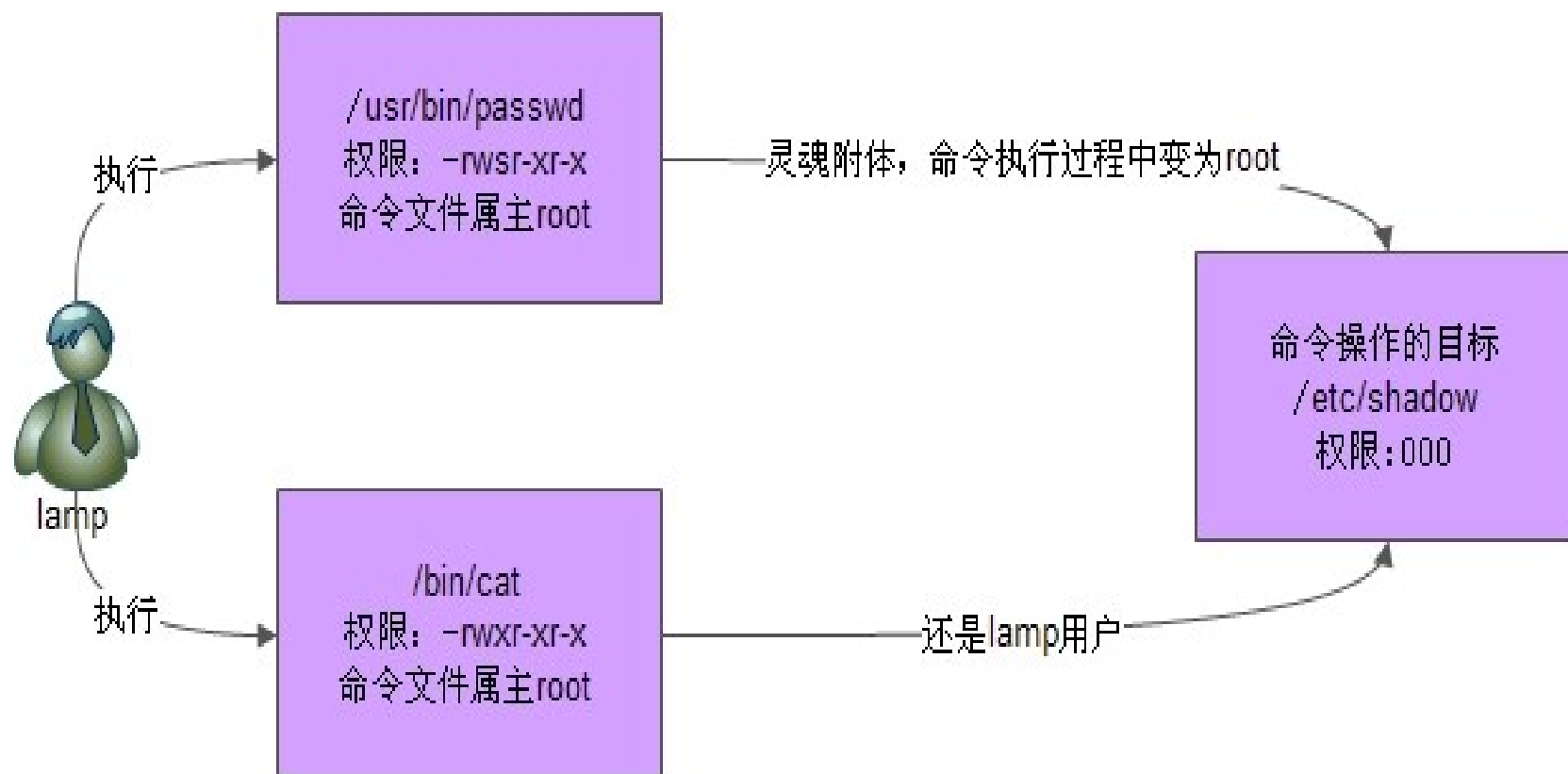
```
[root@localhost ~]# ll /usr/bin/passwd
```

```
-rwsr-xr-x. 1 root root 25980 2月 22 2012 /usr/bin/passwd
```

- ◆ cat命令没有SetUID权限，所以普通用户不能查看/etc/shadow文件内容

```
[root@localhost ~]# ll /bin/cat
```

```
-rwxr-xr-x 1 root root 47976 6月 22 2012 /bin/cat
```



## 2、设定SetUID的方法

### ◆ 4代表SUID

- `chmod 4755 文件名`
- `chmod u+s 文件名`



## 3、取消SetUID的方法

- ◆ `chmod 755 文件名`
- ◆ `chmod u-s 文件名`

## 4、危险的SetUID

- ◆ 关键目录应严格控制写权限。比如“/”、“/usr”等
- ◆ 用户的密码设置要严格遵守密码三原则
- ◆ 对系统中默认应该具有SetUID权限的文件作一列表，定时检查有没有这之外的文件被设置了SetUID权限



扫描上面的二维码  
关注兄弟连官方微信账号

兄弟连官方网址：[www.lampbrother.net](http://www.lampbrother.net)