

【作业3】利用SetUID实现访问权限管理

唐亚周 519021910804

你在为一家审计代理处工作，调查一家公司是否存在诈骗行为。为了这个目的，你需要阅读这家公司在Unix系统中的所有文件。公司系统管理者为了保护系统的可靠性，必须保证审计者可以阅读系统中所有的文件，但不能改写或删除文件。

利用SetUID特性，系统管理员如何实现该诉求？

提示：审计员在Unix系统下使用cat命令查看公司文件内容

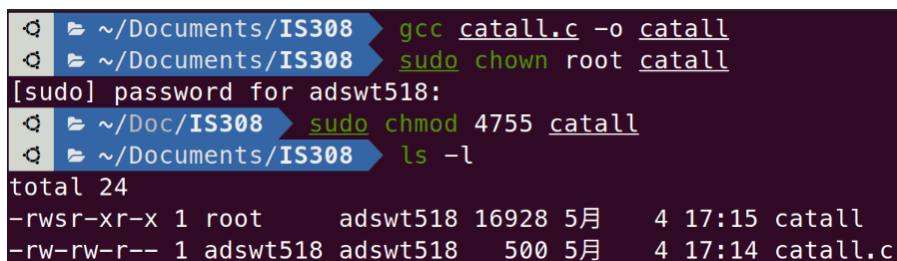
1 代码

我在查阅资料¹后，编写程序如下：

```
1 #include <stdio.h>
2 #include <unistd.h>
3
4 int main(int argc, char *argv[])
5 {
6     char *v[3];
7     if(argc < 2) {
8         printf("Please type a file name.\n");
9         return 1;
10    }
11    v[0] = "/bin/cat"; v[1] = argv[1]; v[2] = NULL;
12
13    execve(v[0], v, NULL);
14
15    return 0 ;
16 }
```

2 测试

首先将上述程序编译，然后将其所有者设置为 root 用户，权限设置为 4755。这样它就成了一个 set-uid 程序。当其他用户执行它时，可以获得 root 用户的权限。



```
~/Documents/IS308 ➤ gcc catall.c -o catall
~/Documents/IS308 ➤ sudo chown root catall
[sudo] password for adswt518:
~/Doc/IS308 ➤ sudo chmod 4755 catall
~/Documents/IS308 ➤ ls -l
total 24
-rwsr-xr-x 1 root      adswt518 16928 5月   4 17:15 catall
-rw-rw-r-- 1 adswt518 adswt518  500 5月   4 17:14 catall.c
```

然后我们使用 root 用户在 /root 目录下创建一个文件 `file.txt`，将其内容设置为“hello world”，并将其权限设置为 700，即 root 用户拥有全部权限，但普通用户任何权限都没有。注意不能在普通用户的 home 目录创建该文件，否则即是设置为无法删除，普通用户依然能够删除该文件。

```
root@lithium:~# touch file.txt
root@lithium:~# echo "hello world" >> file.txt
root@lithium:~# chmod 700 file.txt
root@lithium:~# ls -l file.txt
-rwx----- 1 root root 12 5月  4 17:39 file.txt
```

然后我们切换到普通用户，尝试读取该文件，发现没有权限。但如果我们使用刚刚编写的 set-uid 程序读取该文件，则发现可以读取。同时普通用户尽管使用该 set-uid 程序，也不能对该文件进行修改或删除。

```
~/Documents/IS308 > cat /root/file.txt
cat: /root/file.txt: Permission denied
~/Documents/IS308 > ./catall /root/file.txt
hello world
```

1. https://blog.csdn.net/qq_51927659/article/details/122765563