Windows 系统安全小结

Windows 用户相关命令及隐藏用户：

a. 查看所有用户： net users

b. 查看指定用户 user1： net user user1

c. 添加指定用户 user1： net user user1 password1 /add

d. 删除指定用户 user1： net user user1 /del

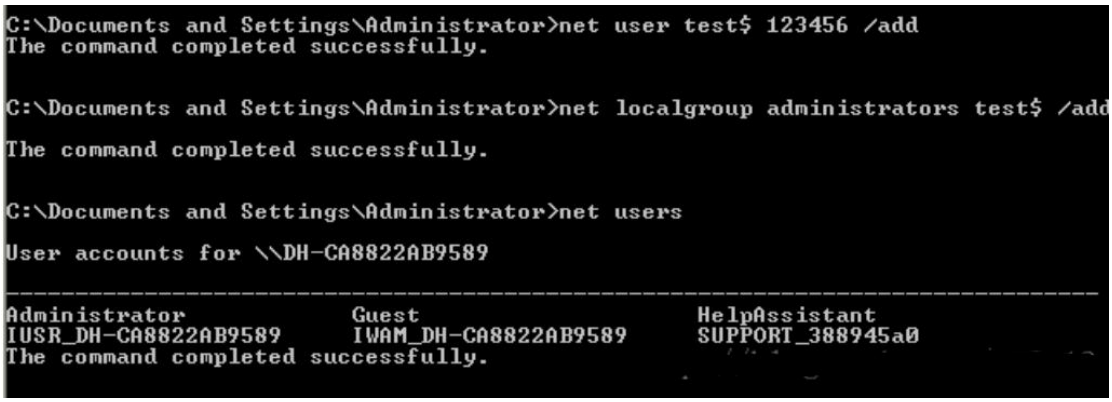
简单地隐藏用户：

添加隐藏用户 test（在账户名后面添加$）：

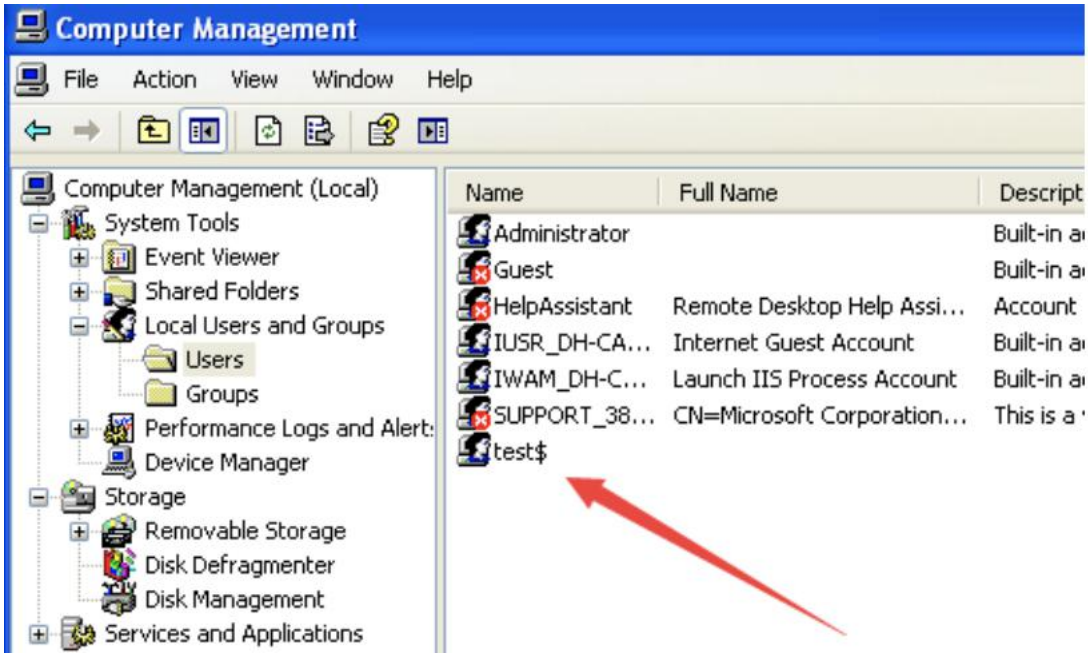
net user test$ /add

net localgroup administrators test$ 123456 /add

这样在命令行下是看不到的：

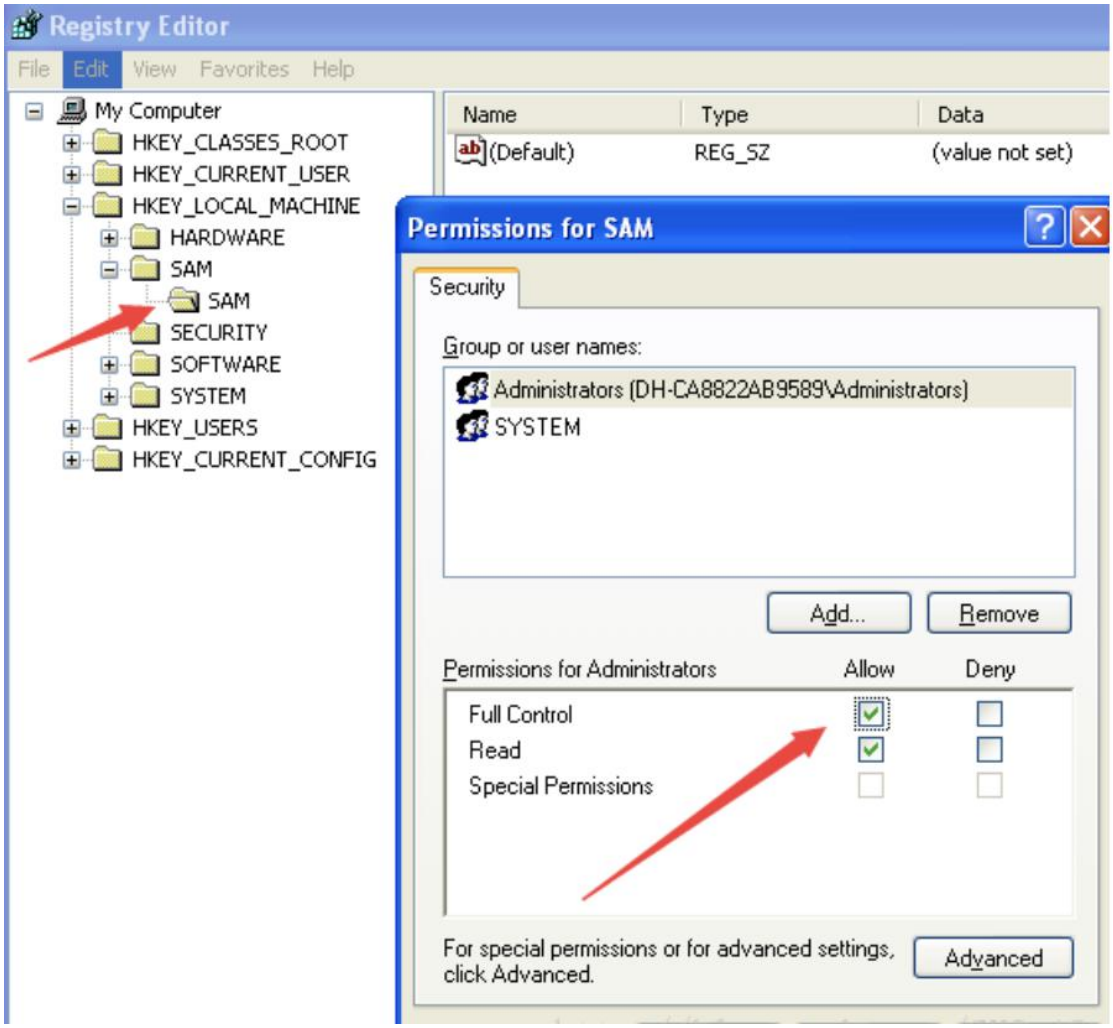


但是在右键“我的电脑”>管理>用户 中却可以看到，即没有很好地隐藏起来：

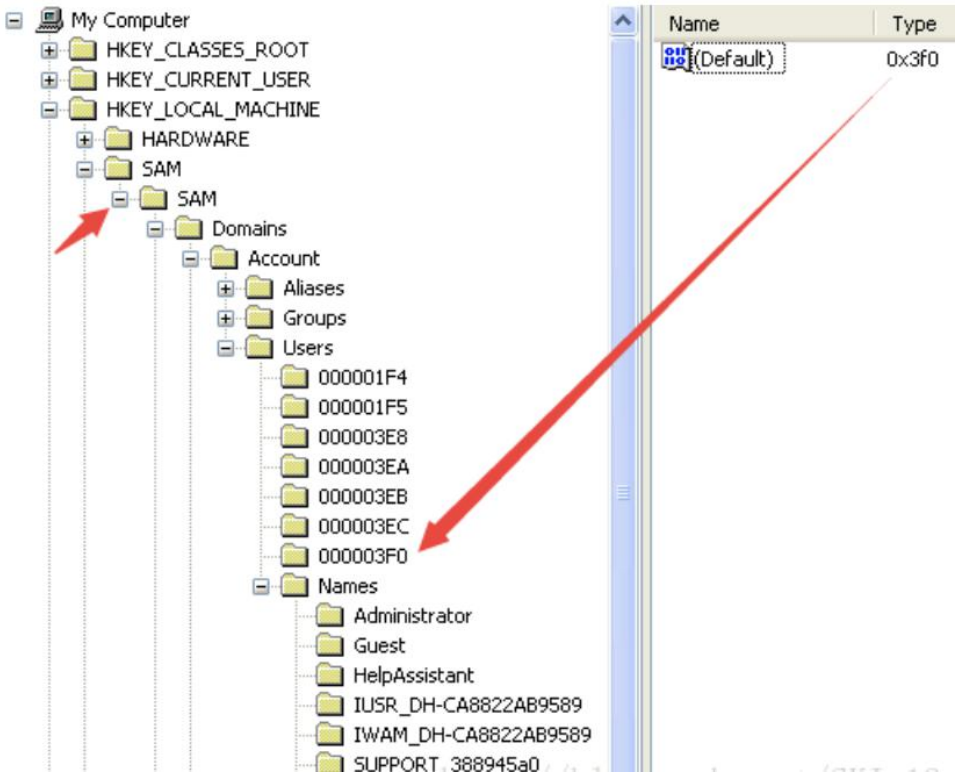


通过注册表隐藏用户：

要实现很好的隐藏，需要通过注册表，运行中输入 regedit，然后点击 HKEY_LOCAL_MACHINE>SAM>SAM,，然后添加相应的权限：

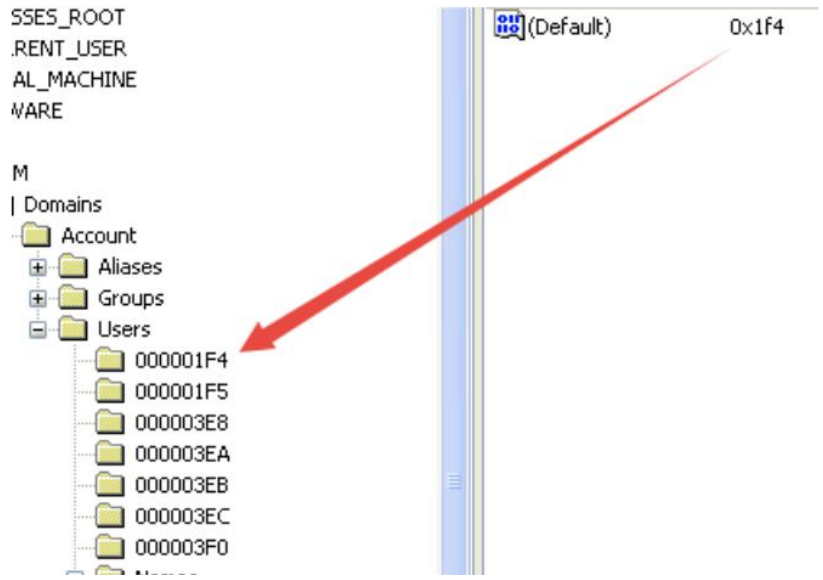


接着重新打开可以看到 SAM 目录签有+号可以打开：



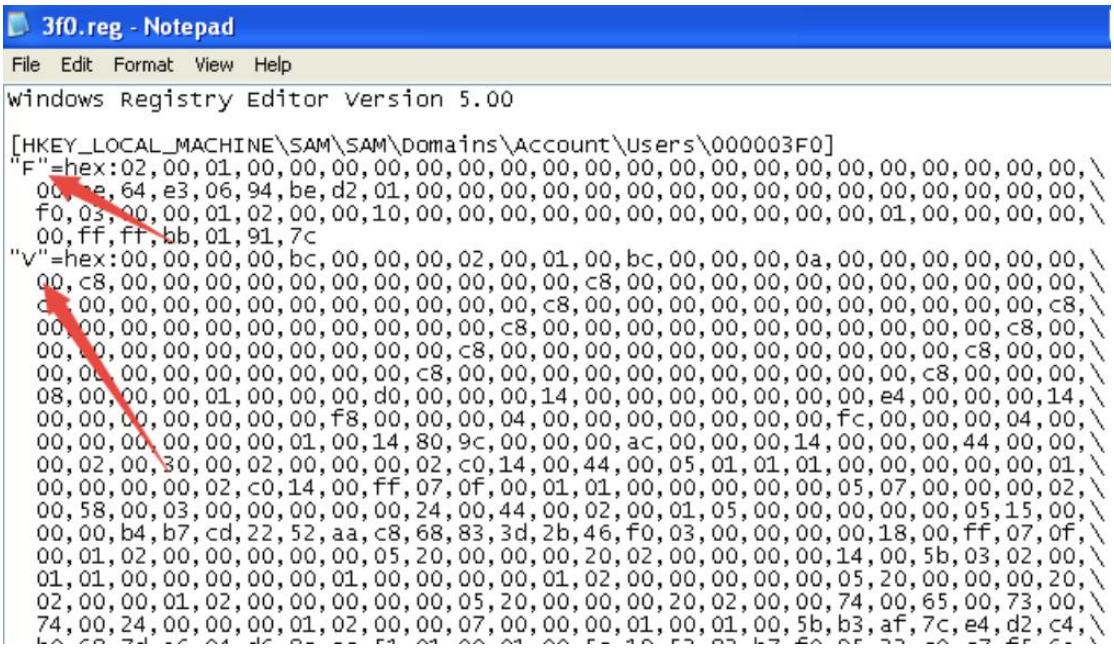
对 test$和 0x3F0 目录右键导出。

若想给 test$用户赋权，则可以将该用户的键值（例子中为 0x3f0）改为 Administrator 的所对应的键值即可。

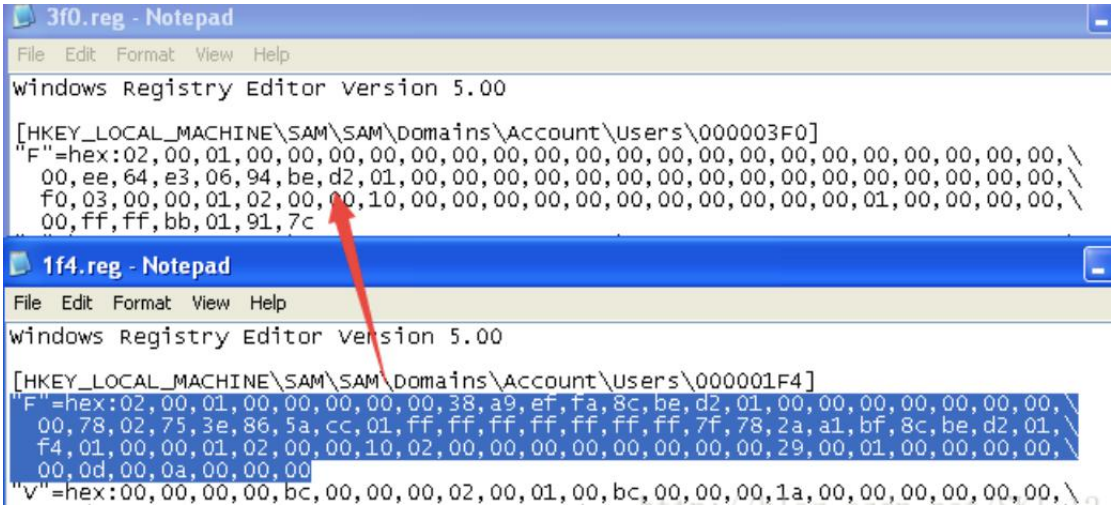


导出 0x1F4 目录。

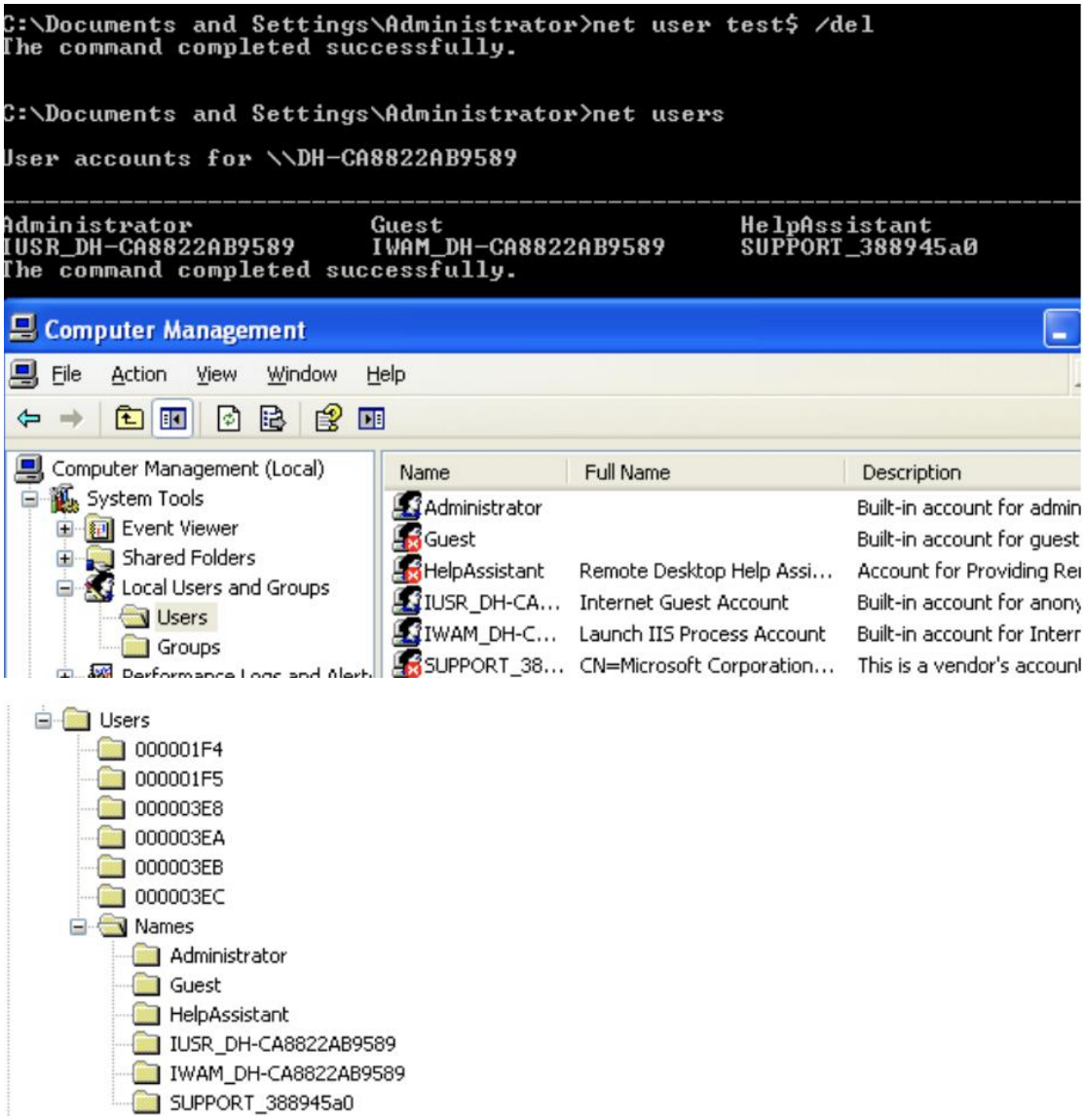
接着打开 0x3F0 目录导出的文件，可以看到 F 表示用户信息，V 表示权限信息：



接着，用 1f4 文件中 F 的键值替换 3f0 中 F 的键值：

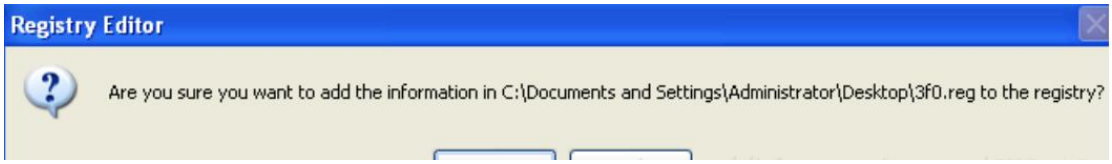


接着在命令行删除 test$用户：

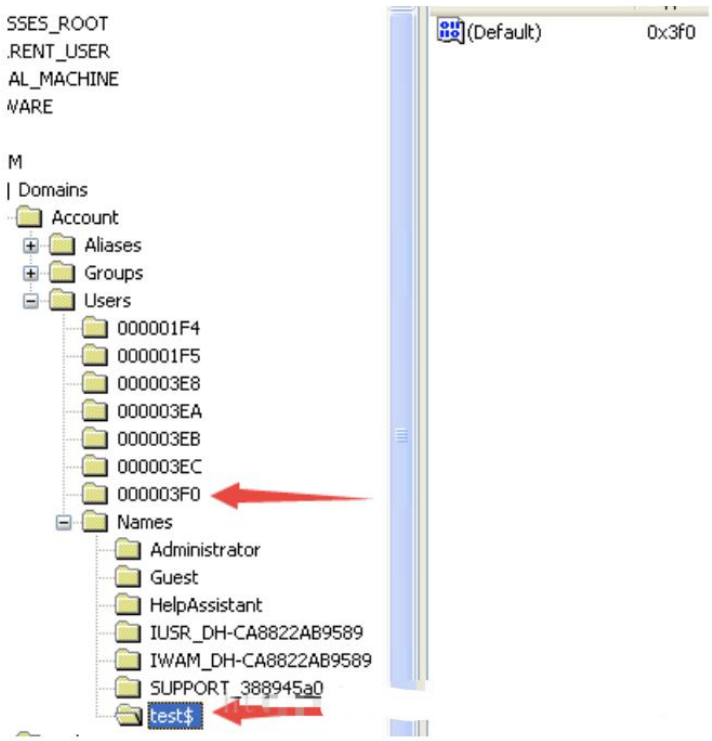


可以看到 test$用户的信息被删除了。

然后双击刚刚修改过的 3f0 文件，提示是否将内容添加进注册表：

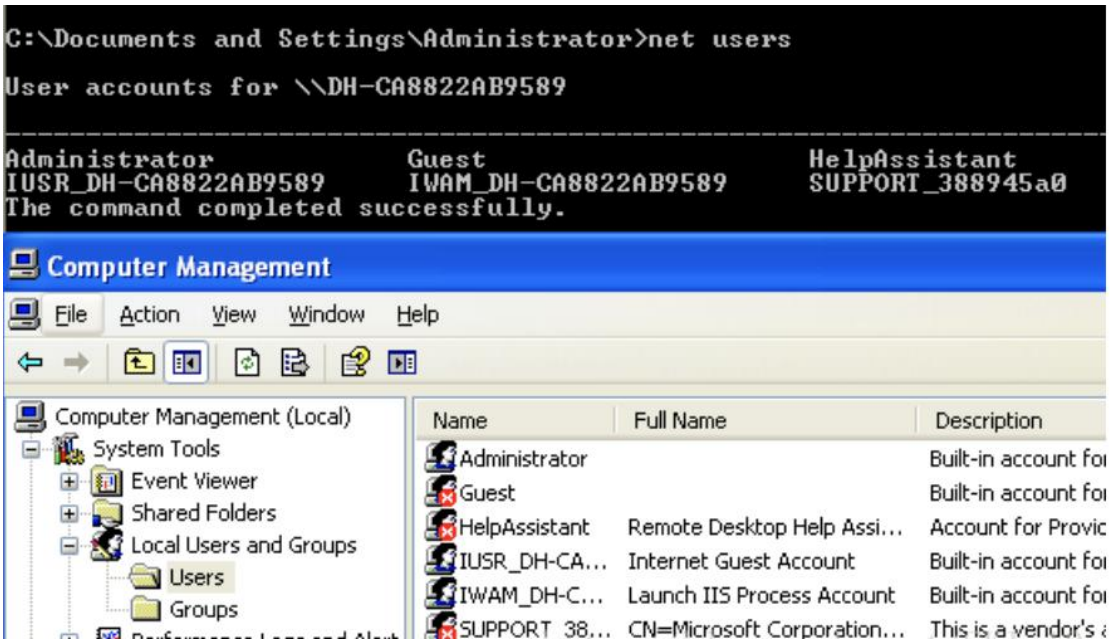


选择 Yes，接着对刚刚导出的 test$.reg 文件进行同样的操作，然后进入注册表中查看：



查看得到刚刚删除的 test$用户又显示出来了。

重新刷新查看计算机管理中的用户和命令行下的 net users 命令，没有显示该用户：



接着注销当前账户后就可以使用 test$用户登录了。

但是上述的方法在注册表中仍然可以查看到，这时可以通过 rootkit 工具实现超级隐藏，具体的操作可以网上查相应的 rootkit 工具的使用。

防御方法：

通过任务管理器查看是否存在用户名后接$的用户，若存在则需要通过杀毒软件找到相应的隐藏文件再将其删除。

Windows 账号克隆：

Windows 账号克隆的整个步骤为：

1、禁用账号 guest

2、改 guest 密码：net user guest pass

3、运行>regedit>HKEY_LOCAL_MACHINE>SAM>SAM>Domains>Account>Users，1F4：Administrator，1F5：guest

4、将 Administrator 中 1F4 的 F 值复制给 guest 中 1F5 的 F 值即可

Windows 服务器权限分析：

常见用户（权限从高到低）：SYSTEM、Administrator、Guest（默认是禁用的）

常见用户组：Administrators（最高权限）、Backup Operators（不如 Administrators 权限高，但差不多）、Guests（与 USER 组权限相同）、Distributed COM Users、Network Configuration Operators、Performance Log Users、Performance Monitor Users、Power Users、Print Operators、Users、IIS_WPG

Windows2003 默认权限：

1、默认只安装静态 HTTP 服务器

2、增强的文件访问控制

3、父目录被禁用

4、坚持最小特权原则

软件捆绑类远控、后门查杀：

1、查看进程：

netstat -an

netstat -ano 多显示一个 PID

tasklist /svc

2、查看服务：

可以使用工具 XueTr

微软服务的描述在最后都是由句号的，而第三方的服务是没有的。

先将 dll 文件删除，然后终止进程关闭服务。