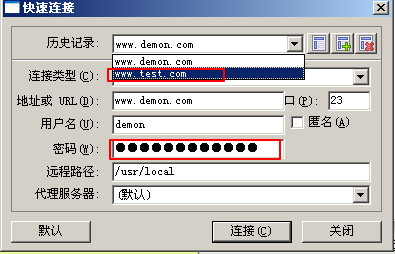
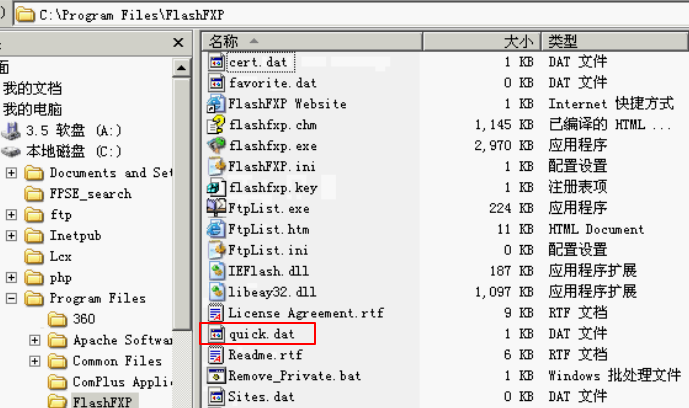
# flashFXP软件获取账号密码

flashFXP软件用于连接FTP服务器的一款客户端软件，每次的登录信息都会自动保存到quick.dat的文件里，因此我们可以利用这个quick.dat文件来获取软件里保存的所有账号密码，然后星号查看器得到密码进一步社工其他账号。



对于flashFXP比较低版本，quick.dat就存放在该软件的安装目录下

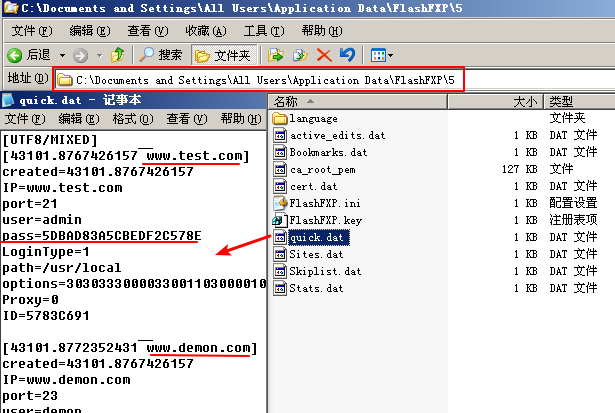


对于版本比较高的，quick.dat存在windows系统的临时文件夹，如下几种可能

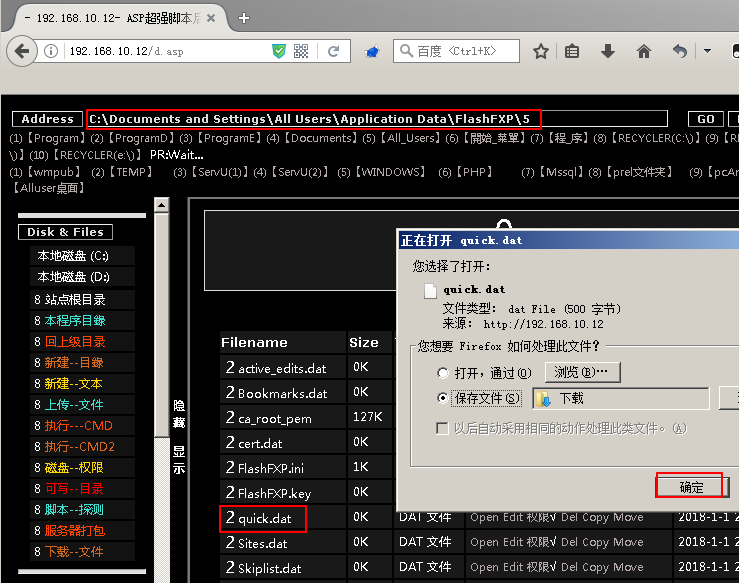
C:\Documents and Settings\All Users\Application Data\FlashFXP\5\quick.dat

C:\Documents and Settings\ OtherUser\Application Data\FlashFXP\5\quick.dat

C:\Documents and Settings\ Administrator\Application Data\FlashFXP\5\quick.dat



通过大马下载该quick.dat文件



然后在攻击者电脑也装一份flashfxp客户端，找到临时文件夹替换其quick.dat即可

另外对于win7系统的临时文件夹是在 c:\programdata下面

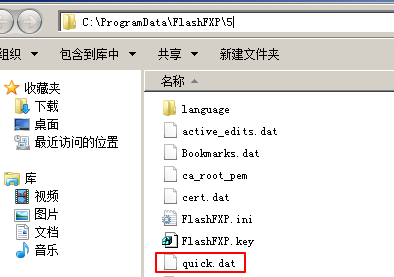
如果不在programdata下，可以参考下面的位置

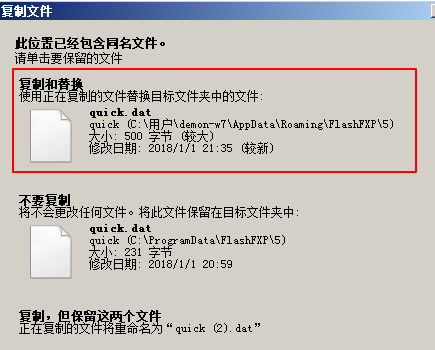
C:\Users\demon-w7\AppData\Roaming\FlashFXP\5

C:\Users\demon-w7\AppData\local\temp\FlashFXP\5

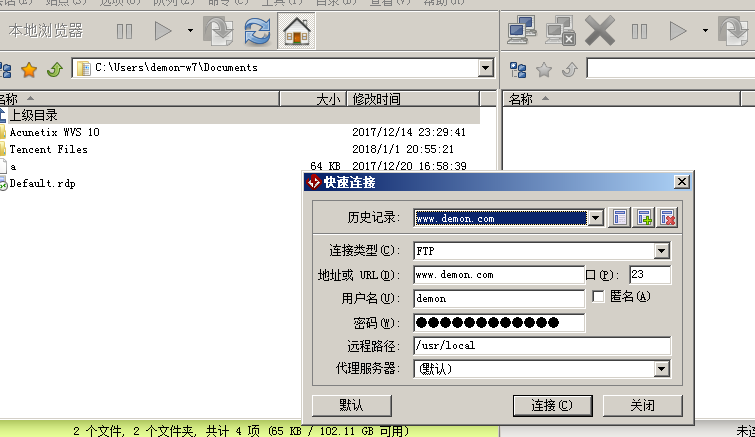
是在找不到用everything搜索也可以







替换后打开软件，在历史记录上就有登录信息，直接登录即可



另外可以用星号查看器查看密码，因为这些密码很有可能也是3389或者telnet和ssh的账号密码

