# filezilla提权

filezilla客户端用于连接FTP服务，filezilla服务端用于充当管理和控制ftp服务器，提权思路：因为filezilla服务器的管理员账号是保存在FileZilla Server Interface.xml文件里（明文），可以通过asp大马访问下载，默认FileZilla 服务器只运行127.0.0.1访问，所以要做端口转发，连上FileZilla Server 后创建ftp普通账号，家目录设置成C:\，给最大权限，然后用FileZilla Client去访问21的ftp服务，登录刚刚创建的账号，用cmd.exe替换c:\windows\system32\sethc.exe

接着mstsc服务器，按5次shift键弹出shell，即可创建超级管理员账号。

实验步骤

1. 读取FileZilla Server Interface.xml 文件，拿到管理员账号密码
2. 上传lcx.exe，做端口转发
3. 连FileZilla Server创建FTP用户，家目录为C盘，权限给最大
4. 用FileZilla Client连FTP服务，用cmd.exe替换c:\windows\system32\sethc.exe
5. 用mstsc按5次shift键弹shell创建超级管理用户，提权成功

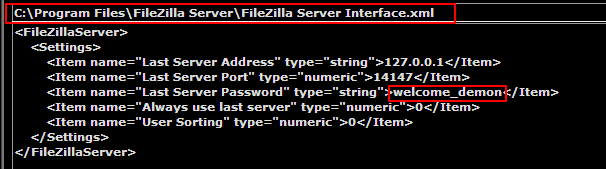
准备环境

win2003靶机安装FileZilla Server 0.9.42，如果是其他版本可能会不兼容报错

win7攻击机安装FileZillaClient3.29 和FileZilla Server 0.9.42因为要连接器

开始实验

通过大马找到FileZilla Server的软件安装目录下，里头有xml文件，编辑即可拿到密码



查看可写目录，上传lcx和cmd做端口转发



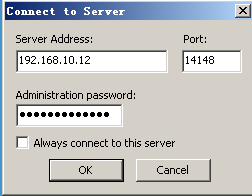


echo. | c:\recycler\lcx.exe -tran 14148 127.0.0.1 14147

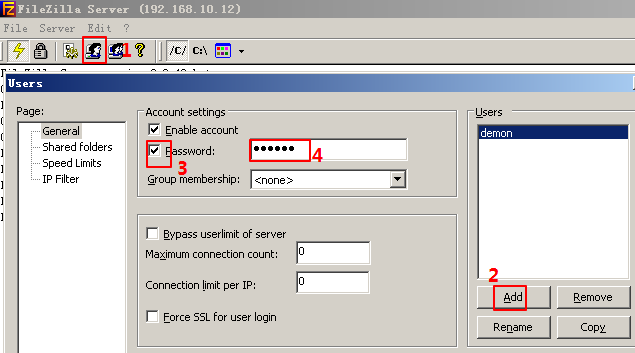


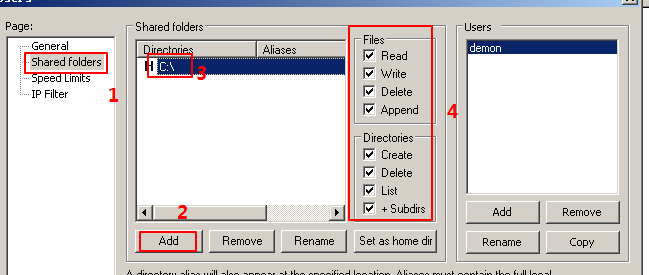
点击转发后浏览器会卡住，关掉重新netstat -an查看端口即可，转发好后连filezilla server

在攻击者这边也要转filezilla server，这样才有连接器FileZilla Server Interface



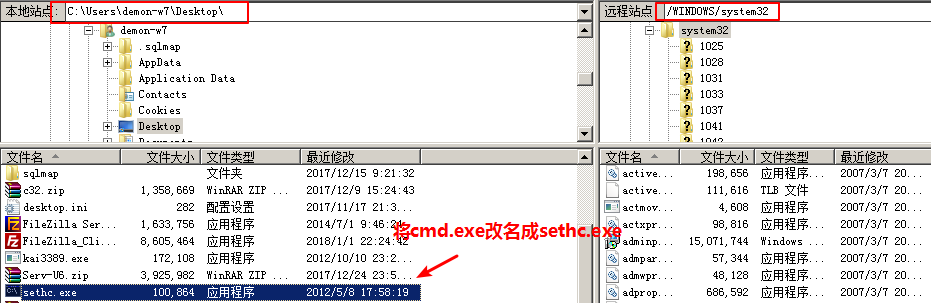
创建一个FTP用户，设置权限和设C盘为家目录





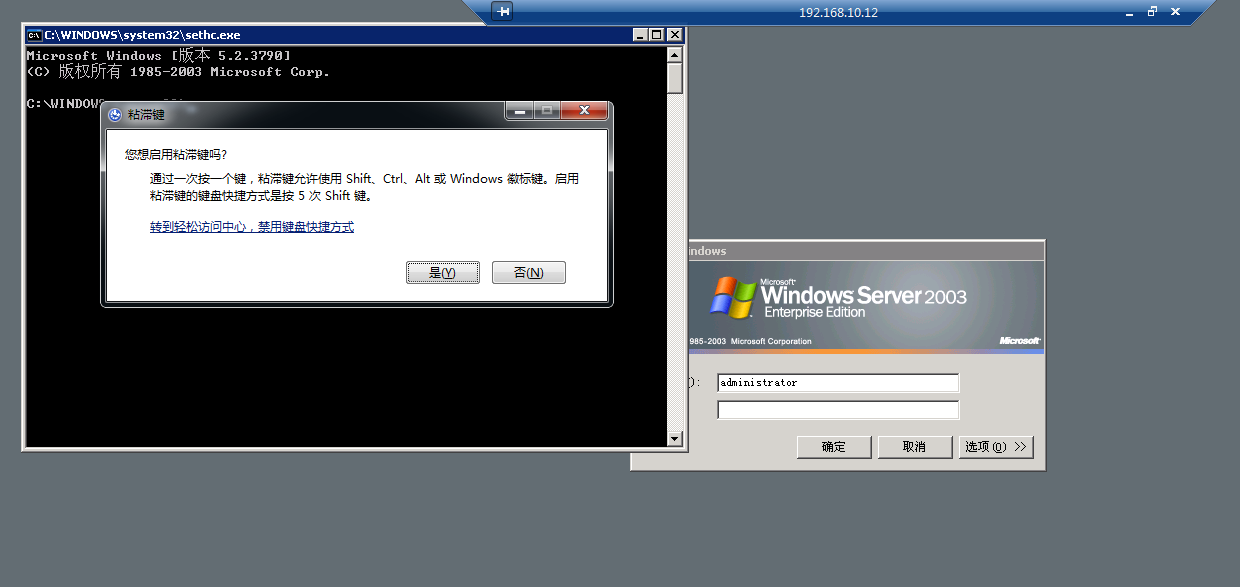
然后用Filezilla客户端去连FTP服务，用刚刚创建的账号登录



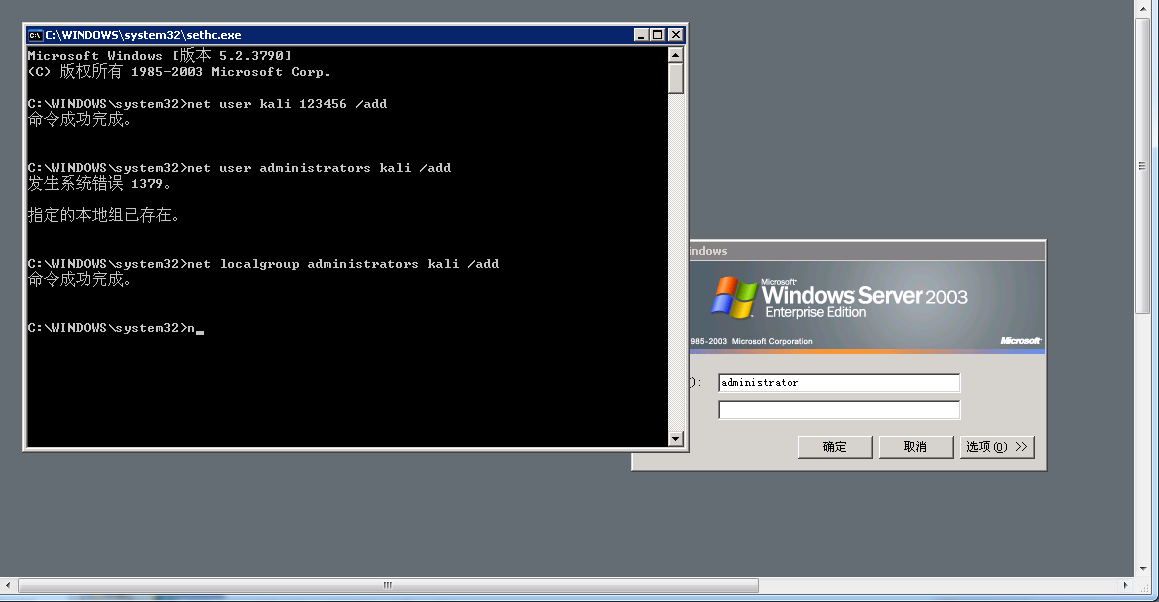


改名cmd.exe然后上传到ftp服务的/WINDOWS/system32目录下覆盖原有的

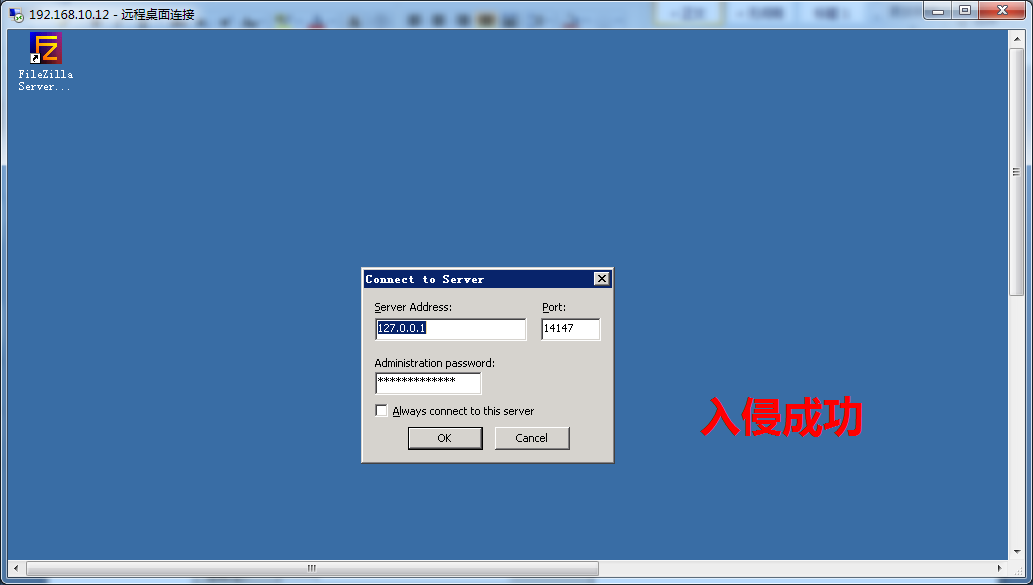
然后用mstsc远程登录按5次shift，弹出shell创建超级用户连接即可



创建超级管理员账号







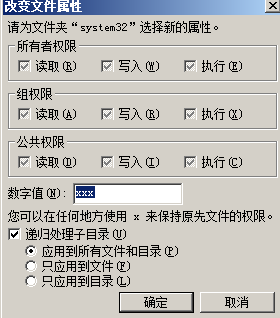
实验的时候出了一些问题：

问题一：上传sethc.exe假成功

上传覆盖后提示成功，但是过一会有又自动变回去了，感觉是没有成功的

后面检查修改了两个小细节，在创建ftp用户设定家目录的时候写的是C:

修改后写成C:\，其次就是在filezilla客户端上右键windows目录权限遍历批量给



问题二：上传成功了，但是按5次shift弹不出shell

分析原因可能是替换成sethc.exe的cmd.exe必须是win2003原版的，其他版本的可能不行

解决：客户端下载c:\windows\system32\cmd.exe下来改名成sethc.exe再重新上传覆盖就行