# Win2003远程桌面服务爆破

环境准备：

win7 (攻击) win2003(服务器)

## 首先在win2003启动下面的服务，开启3389远程桌面服务

### 创建 .bat 文件输入下面内容：

scconfig LmHosts start= auto

sc config RpcLocator start= auto

sc configNtlmSsp start= auto

sc config lanmanserver start= auto

sc configSharedAccess start= disabled

net start LmHosts 2>nul

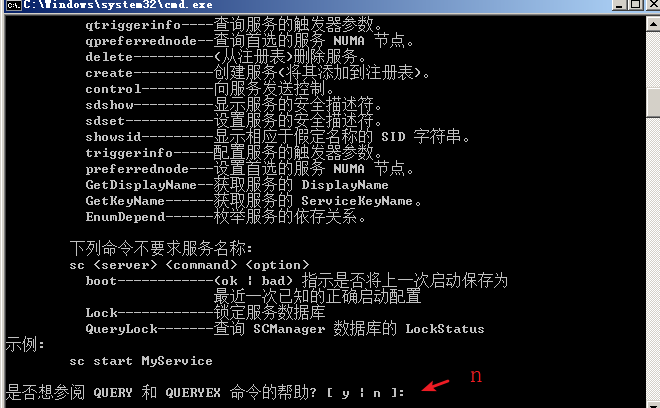
net startRpcLocator 2>nul

net start NtlmSsp 2>nul

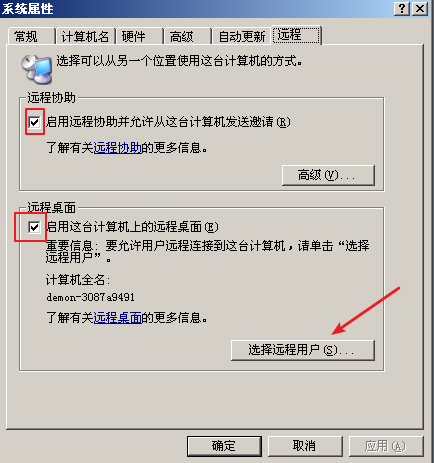
net start lanmanserver2>nul

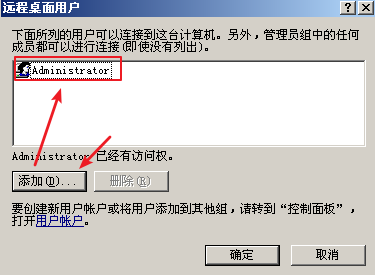
net stop SharedAccess >nul 2>nul

### 双击运行，没有的话跳过即可

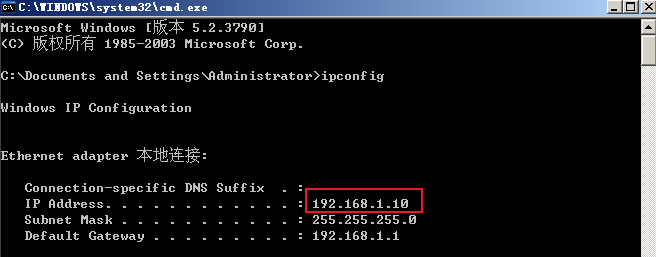


### 启动服务，配置登陆用户

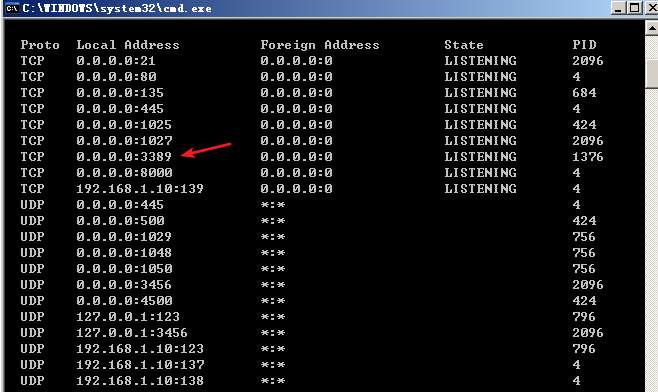




### 查看服务器IP地址



### 查看端口是否启动

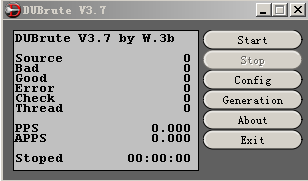


## 然后在win7准备工具对win2003远程服务进行爆破

这里使用工具：DUBrute 图标如下：



### 工具介绍



Source表示“源”。

Bad表示“失败的”

Good表示“成功的”

Error表示“错误的”

Check表示：“检测”

Thread表示“线程”

Start表示“开始”

Stop表示“停止”

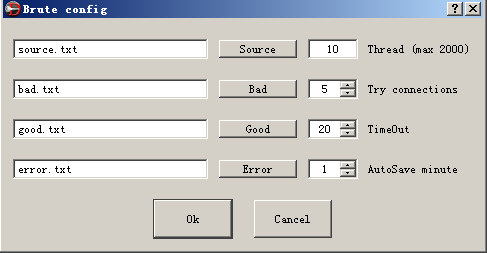
Config表示“配置”

Generation 表示“生成”

About表示“关于”

Exit表示“退出”

大概重要的翻译完了，后面配置详细的设置参数，直接打开config



source.txt 破解参数文件

bat.txt 破解失败的文件

good.txt 破解成功的文件

error.txt 破解出错的文件

thread 破解开启的线程数

try connections 尝试连接数

timeout 超时

autoSave minute 自动保存时间(分)

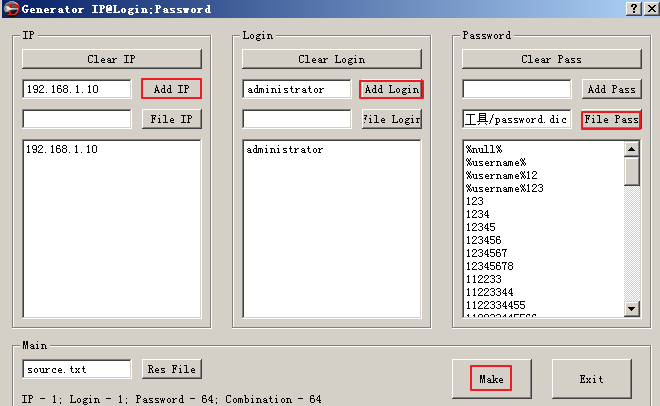
完成以上配置后,点击OK 然后回到初始界面点击Generation设置帐号密码以及IP信息。

打开后会发现有三列需要添加的东西:

* 第一列中是需要爆破的IP，我们直接点击File IP导入IPS下的所有IP
* 第二列Login是登陆账号，可直接选添加用户名，也可导入Username的字典
* 第三列Password，选File pass导入我们的3389密码字典。最后点击made，退出界面

### 开始破解

IP填写WIN2003的IP地址，账号administrator 准备一份密码字典：



密码字典另存为文本文件，内容如下：

%null%

%username%

%username%12

%username%123

123

1234

12345

123456

1234567

12345678

112233

11223344

1122334455

112233445566

88888888

654321

54321

111

000000

00000000

11111111

88888888

pass

passwd

password

database

admin

root

abcd

abc123

secret

oracle

sybase

test

123qwe

server

computer

Internet

super

123asd

!@#$%^&\*

administrator

ihavenopass

godblessyou

!@#$%^&\*()

enable

xp

2002

2600

0

1

111111

121212

123123

1234qwer

123abc

007

abc

alpha

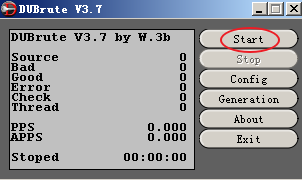
admin

administrator

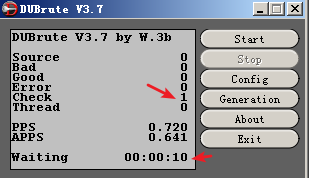
admin123

4rfvgy7

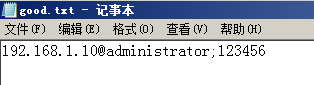
保存后点击破解软件上的file pass导入密码字典即可，最后单击make 和 exit



点击开始，当破解成功后good字段会显示为1，顶部显示所话的时间



双击good.txt文件，可以看到里边保存着win2003账号密码



### 登陆测试

win + R 输入mstsc，账号输administrator 密码输 123456



