# winver（常用）

检查windows版本

# write

写字板

# wiaacmgr

扫描仪和照相机向导

# mspaint

画图板

# mstsc（常用）

远程桌面连接

# mmc（常用）

打开控制台

# cls（常用）

清空命令行

# notepad

打开记事本

# devmgmt.msc

设备管理器

# secpol.msc

本地安全策略

# services.msc（常用）

本地服务设置

# taskmgr

任务管理器

# eventvwr

事件查看器

# explorer（常用）

打开资源管理器

# regedit.exe(或者是regedit) （常用）

注册表

# calc（常用）

计算器

# odbcad32

ODBC数据库管理器

# logoff

注销命令

# gpedit.msc

组策略

# shutdown -s

关机

# control

打开控制面板

# control system

打开系统属性

# control sysdm.cpl

打开系统高级属性

# control wscui.cpl

打开操作中心

# control firewall.cpl

打开windows防火墙

# control mouse

设置鼠标属性

# control fonts

设置字体

# control color

设置窗口颜色/外观

# control appwiz.cpl

开启添加/删除程序

# ping（常用）

## 基本概念

用来检查网络是否畅通或者网络连接速度的命令，原理是网络上的机器都有唯一确定的IP地址，我们给目标IP地址发送一个数据包，对方就要返回一个同样大小的数据包，根据返回的数据包我们可以确定目标主机的存在，可以初步判断目标主机的操作系统。在dos窗口中输入ping /?显示该命令的语法。

## 语法



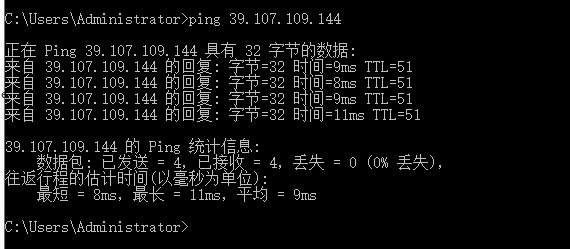
-t 表示将不断的向目标IP发送数据包，直到我们强制停止。

-l 定义发送数据包的大小，默认是32字节，我们可以利用它最大定义到65500，结合-t一起使用，会有很好的效果。

-n 定义向目标IP发送数据包的次数，默认为3次，如果网络速度较慢，3次对我们来说浪费了不少时间，因为我们的目标是仅仅判断目标IP是否存在，那么就定义一次。

ping命令不一定非的ping IP地址，也可以直接ping 主机域名，这样就可以得到主机的IP地址。

## 举例



time=2表示从发出数据包到接受到返回数据包所用的时间是2秒，从这里可以判断网络连接速度的大小，从TTL的返回值可以初步判断被ping主机的操作系统，之所以说“初步判断”是因为这个值是可以修改的，这里TTL=32表示操作系统可能是win98的，如果TTL=128，则表示目标主机可能是Win2000；如果TTL=250，则目标主机可能是Unix。利用ping命令可以快速查找局域网故障，可以快速搜索最快的QQ服务器，可以对别人进行ping攻击，这些就大家自己发挥了。

# nbtstat

## 基本概念

该命令使用TCP/IP上的NetBios显示协议统计和当前TCP/IP连接，使用这个命令你可以得到远程主机的NETBIOS信息，比如用户名、所属的工作组、网卡的MAC地址。

-a 使用这个参数，只要你知道了远程主机的机器名称，就可以得到它的NETBIOS信息。

-A 这个参数也可以得到远程主机的NETBIOS信息，需要你知道它的IP地址。

-n 列出本地机器的NETBIOS信息。

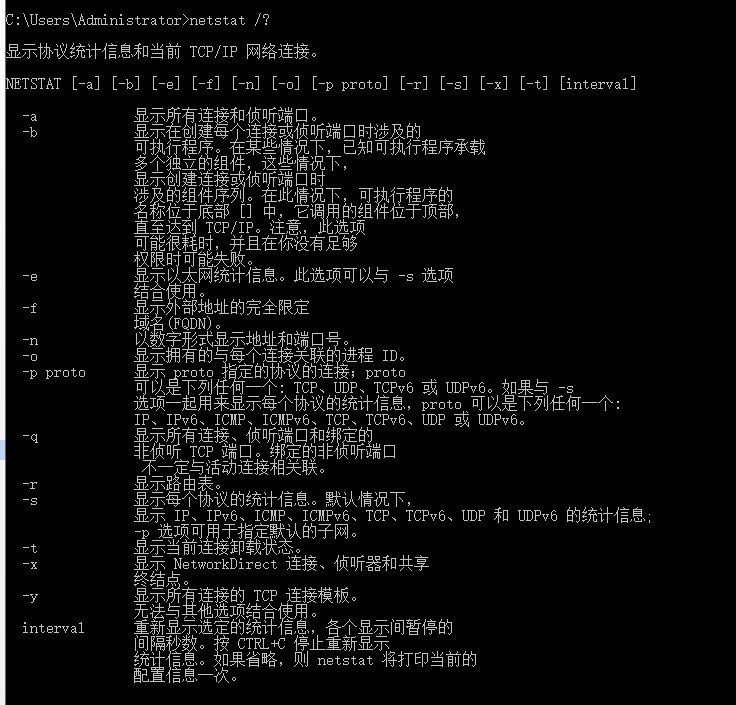
当得到了对方的IP或者是机器名的时候，就可以用nbtstat命令进一步得到对方的信息了。

# netstat（常用）

## 基本概念

这是一个用来查看网络状态的命令，操作简单功能强大。

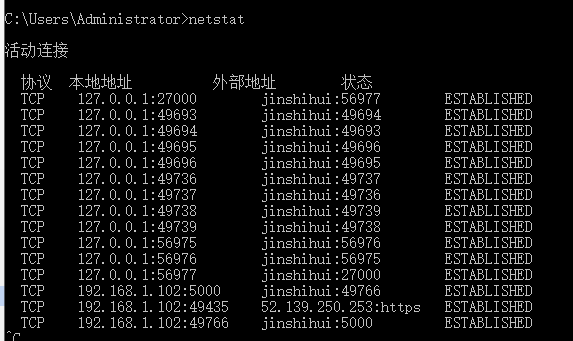
## 语法



-a 查看本地机器的所有开放端口，可以有效发现和预防木马，可以直到机器所开的服务等信息。用法：netstat -a IP

-r 列出当前的路由信息，告诉我们本地机器的网关、子网掩码等信息，用法：netstat -r IP。

## 示例



# tracert

跟踪路由信息，使用此命令可以查看数据从本地机器传输到目标主机经过的所有途径，这对我们了解网络布局和结构很有帮助。

# net（常用）

## 基本概念

网络命令，这个命令非常重要，必须掌握。有关帮助输入net /?。

## 语法



## （1）net view

使用此命令可以查看远程主机的所有共享资源，命令格式是：net view \IP

## （2）net start

启动远程主机上的服务。用法是：net start servername

## （3）net stop

停掉服务 用法是：net stop servername

## （4）net user

查看和账户有关的情况，包括新建账户、删除账户、查看特定账户、激活账户、账户禁用等。

### 创建用户

net user 用户名 密码 /add

### 删除用户

net user 用户名 /del

### 禁用用户

net user 用户名 /active:no

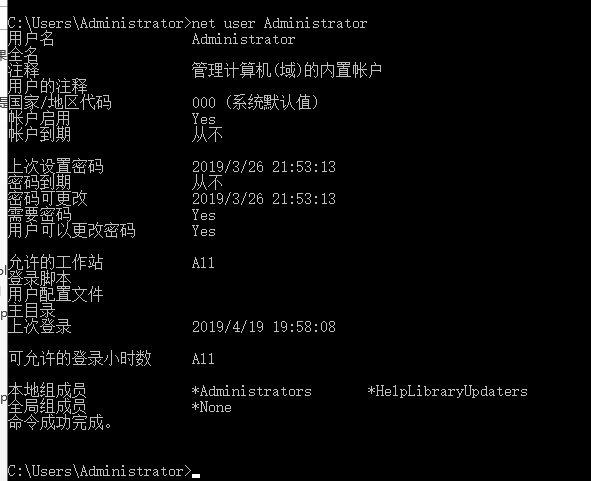
### 激活用户

net user 用户名 /active:yes

### 查看用户（常用）

net user 用户名

示例：

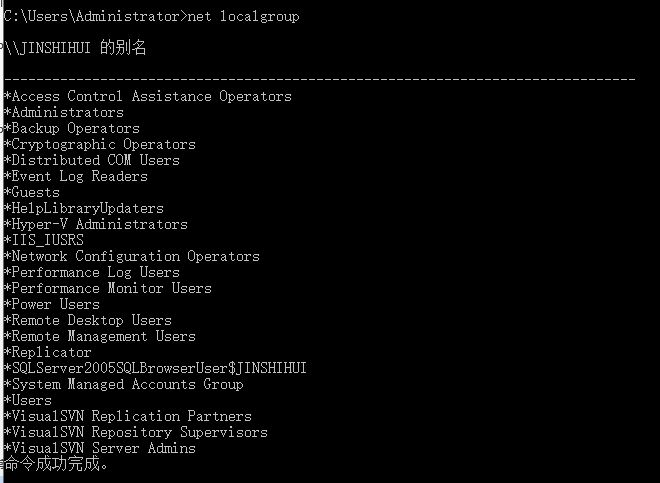


## net localgroup

查看所有和用户组有关的信息和进行相关操作，键入不带参数的net localgroup即列出当前所有的用户组。在入侵过程中，我们一般利用它来把某个账户提升为administrator组账户，我们可以利用这个账户就可以控制远程主机了。

用法：net localgroup groupname username /add

示例：



## net time

这个命令可以查看远程主机当前的时间。用法：net time \\IP



# telnet（常用）

## 基本概念

功能强大的远程登录命令，操作简单，如同操作自己的机器一样。首先键入telnet，再键入help查看帮助信息。然后在提示符下键入open IP回车，出现了登录窗口，输入合法的用户名和密码，这里密码是不显示的，当输入用户名和密码正确后就成功建立了telnet连接。

## 语法

c 关闭当前的连接

d 显示操作参数

o 连接到主机（默认端口是23）

q 退出telnet

set 设置选项

sen 将字符串发送到服务器

st 打印状态信息

u 解除设置选项

？/h 打印帮助信息

# ftp

## 基本概念

连接远程ftp服务器的主机，输入ftp，进入ftp命令提示符下，输入open IP地址就可以登录了，接下来是输入用户名和密码。

## 语法

dir 用于查看服务器上的文件。

cd 进入到某个文件夹

get 下载文件到本地机器

put 上传文件到远程服务器

delete 删除远程ftp服务器上的文件

quit 退出当前连接

bye 退出当前连接

## 示例

1、通过FTP下载文件：

（1）进入cmd命令窗口。



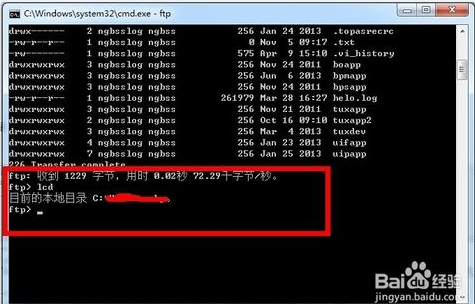
（2）输入"ftp"切换到到ftp下面.然后输入"open 服务器地址".点击回车键.会提示你输入用户名和密码.



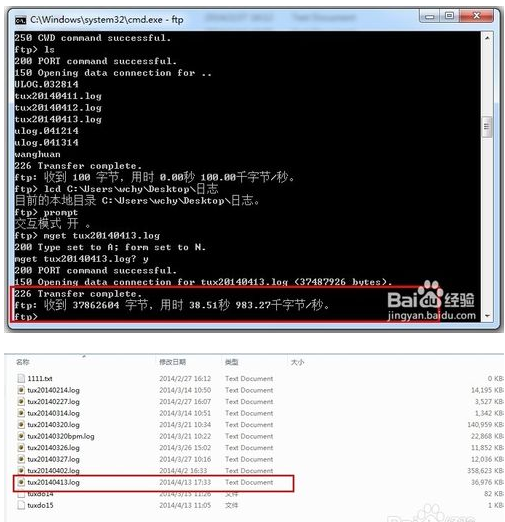


（3）登陆成功后.输入"cd"命令.会显示"远程目录",输入"dir"命令会显示目录下的文件,权限等相关信息.可以通过"cd 文件名"命令进入到要下载的文件目录下.然后输入"ls"命令 显示文件夹下的所有文件.

（4）输入"lcd 本地文件目录"(就是要下载到那个文件夹下 就输入那个目录,如果不输入就是默认c盘的当前系统用户目录下)



（5）输入"prompt"命令(打开交互模式),最后输入"get 服务器上要下载的文件名",回车键.这样就可以进行下载了.看到"Transfer complete"就表示下载成功了.到本地路径下就能看到下载的文件了.



2、通过FTP上传文件

（1）进入dos命令，连接远程服务器：ftp 远程服务器地址。

（2）put 上传文件的地址，回车，屏幕会提示你传输完毕。

（3）dir 回车，查看文件是否上传成功。

3、常用的ftp命令

（1）open 连接服务器。

（2）send(put)：上传文件

（3）get：下载文件

（4）mget：下载多个文件

（5）cd：切换目录

（6）dir：查看当前目录下的文件

（7）del：删除文件

（8）mdel：删除多个文件

（9）bye（quit）：中断与服务器的连接

（10）binary：设定以二进制进行传输文件

（11）system：显示远程主机的系统类型

（12）status：显示当前FTP的状态。