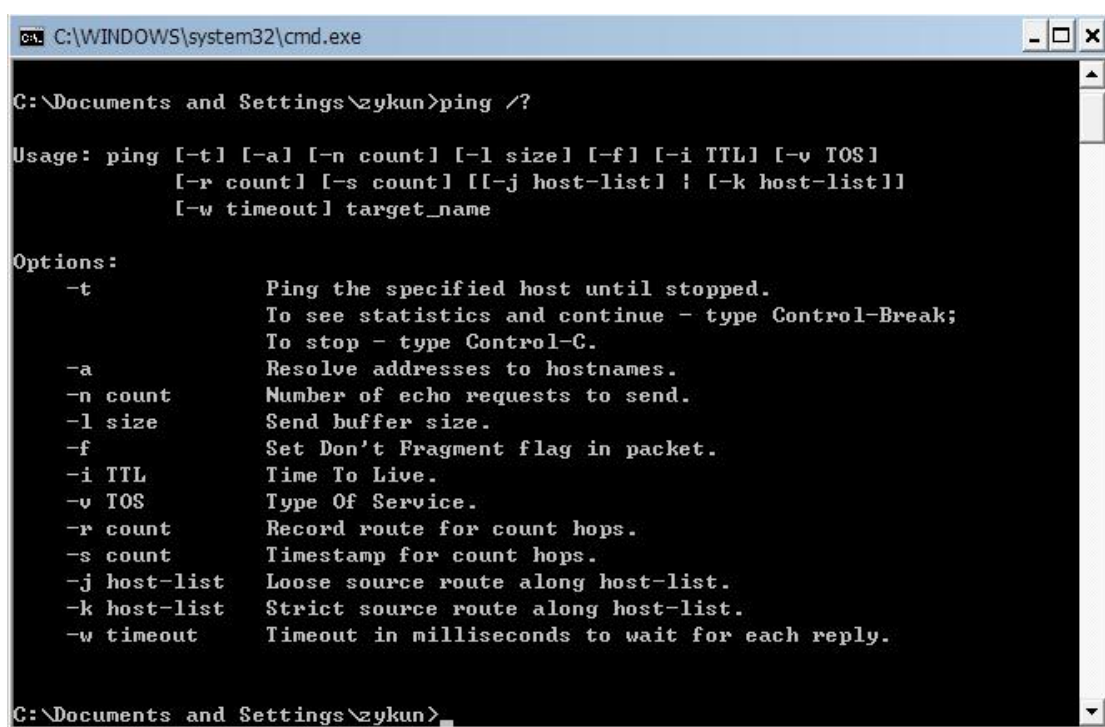


# 管理员必须掌握的常用命令

## 一、ping

它是用来检查网络是否通畅或者网络连接速度的命令。它所利用的原理是这样的：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等。在 DOS 窗口中键入：ping /? 回车。所示如下帮助画面：



```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\zykun>ping /?

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
          [-r count] [-s count] [[-j host-list] ! [-k host-list]]
          [-w timeout] target_name

Options:
    -t          Ping the specified host until stopped.
                To see statistics and continue - type Control-Break;
                To stop - type Control-C.
    -a          Resolve addresses to hostnames.
    -n count    Number of echo requests to send.
    -l size     Send buffer size.
    -f          Set Don't Fragment flag in packet.
    -i TTL      Time To Live.
    -v TOS      Type Of Service.
    -r count    Record route for count hops.
    -s count    Timestamp for count hops.
    -j host-list Loose source route along host-list.
    -k host-list Strict source route along host-list.
    -w timeout  Timeout in milliseconds to wait for each reply.

C:\Documents and Settings\zykun>
```

-t 表示将不间断向目标 IP 发送数据包，直到我们强迫其停止。试想，如果你使用 100M 的宽带接入，而目标 IP 是 56K 的小猫，那么要不了多久，目标 IP 就因为承受不了这么多的数据而掉线，呵呵，一次攻击就这么简单的实现了。

-l 定义发送数据包的大小，默认为 32 字节，我们利用它可以最大定义到 65500 字节。结合上面介绍的-t 参数一起使用，会有更好的效果哦。

-n 定义向目标 IP 发送数据包的次数，默认为 3 次。如果网络速度比较慢，3 次对我们来说也浪费了不少时间，因为现在我们的目的仅仅是判断目标 IP 是否存在，那么就定义为一次吧。

说明一下，如果-t 参数和 -n 参数一起使用，ping 命令就以放在后面的参数为标准，比如"ping IP -t -n 3"，虽然使用了-t 参数，但并不是一直 ping 下去，而是只 ping 3 次。另外，ping 命令不一定非得 ping IP，也可以直接 ping 主机域名，这样就可以得到主机的 IP。

下面我们举个例子来说明一下具体用法。

这里 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

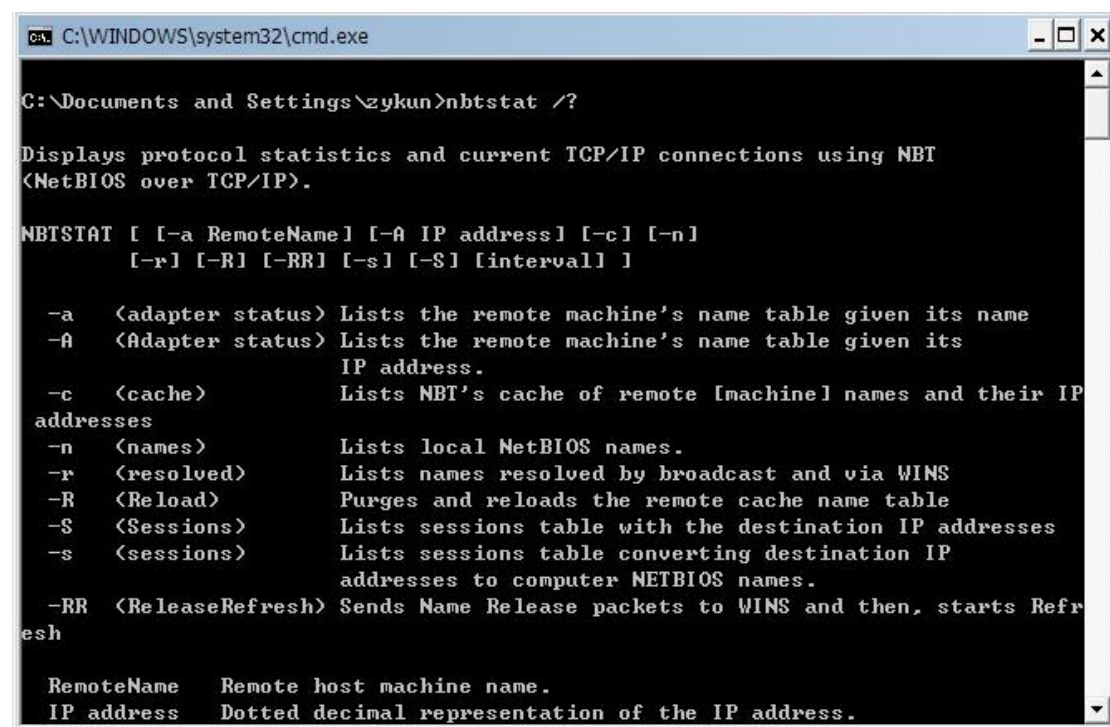
"初步判断"是因为这个值是可以修改的。这里 TTL=32 表示操作系统可能是 win98。

（小知识：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）

至于利用 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.....这些就靠大家自己发挥了。

## 二、nbtstat （查看远程计算机的 MAC 地址）

NBTSTAT 命令可以用来查询网络机器的 NetBIOS 信息及机器的 MAC 地址。另外，它还可以用来消除 NetBIOS 高速缓存器和预加载 LMHOSTS 文件。这个命令在进行安全检查时非常有用。



```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\zykun>nbtstat /?

Displays protocol statistics and current TCP/IP connections using NBT
(NetBIOS over TCP/IP).

NBTSTAT [ [-a RemoteName] [-A IP address] [-c] [-n]
          [-r] [-R] [-RR] [-s] [-S] [interval] ]

-a <adapter status> Lists the remote machine's name table given its name
-A <Adapter status> Lists the remote machine's name table given its
                    IP address.
-c <cache>          Lists NBT's cache of remote [machine] names and their IP
addresses
-n <names>          Lists local NetBIOS names.
-r <resolved>       Lists names resolved by broadcast and via WINS
-R <Reload>         Purges and reloads the remote cache name table
-S <Sessions>       Lists sessions table with the destination IP addresses
-s <sessions>       Lists sessions table converting destination IP
                    addresses to computer NETBIOS names.
-RR <ReleaseRefresh> Sends Name Release packets to WINS and then, starts Refr
esh

RemoteName  Remote host machine name.
IP address  Dotted decimal representation of the IP address.
```

用法：nbtstat [-a RemoteName] [-A IP\_address] [-c] [-n] [-R] [-r] [-S]  
[-s]  
[interval]

参数-a 列出为其主机名提供的远程计算机名字表。

-A 列出为其 IP 地址提供的远程计算机名字表。

-c 列出包括了 IP 地址的远程名字高速缓存器。

-n 列出本地 NetBIOS 名字。

-r 列出通过广播和 WINS 解析的名字。

-R 消除和重新加载远程高速缓存器名字表。

-S 列出有目的地 IP 地址的会话表。

-s 列出会话表对话。

NBTSTAT 生成的列标题具有以下含义：

**Input**

接收到的字节数。

**Output**

发出的字节数。

**In/Out**

无论是从计算机（出站）还是从另一个系统连接到本地计算机（入站）。

**Life**

在计算机消除名字表高速缓存表目前“度过”的时间。

**Local Name**

为连接提供的本地 NetBIOS 名字。

**Remote Host**

远程主机的名字或 IP 地址。

**Type**

一个名字可以具备两个类型之一：**unique or group**

在 16 个字符的 NetBIOS 名中，最后一个字节往往有具体含义，因为同一个名可以在同一台计算机上出现多次。这表明该名字的最后字节被转换成了 16 进制。

**State**

NetBIOS 连接将在下列“状态”（任何一个）中显示：

状态含义：

**Accepting:** 进入连接正在进行中。

**Associated:** 连接的端点已经建立，计算机已经与 IP 地址联系起来。

**Connected:** 这是一个好的状态！它表明您被连接到远程资源上。

**Connecting:** 您的会话试着解析目的地资源的名称-IP 地址映射。

**Disconnected:** 您的计算机请求断开，并等待远程计算机作出这样的反应。

**Disconnecting:** 您的连接正在结束。

**Idle:** 远程计算机在当前会话中已经打开，但现在没有接受连接。

**Inbound:** 入站会话试着连接。

**Listening:** 远程计算机可用。

**Outbound:** 您的会话正在建立 TCP 连接。

**Reconnecting:** 如果第一次连接失败，就会显示这个状态，表示试着重新连接。

下面是一台机器的 NBTSTAT 反应样本：

```
C:\>nbtstat CA x.x.x.x
```

NetBIOS Remote Machine Name Table

Name Type Status

DATARAT <00> UNIQUE Registered

R9LABS <00> GROUP Registered

DATARAT <20> UNIQUE Registered

DATARAT <03> UNIQUE Registered

GHOST <03> UNIFQUE Registered

DATARAT <01> UNIQUE Registered

MAC Address = 00-00-00-00-00-00

您通过下表能掌握有关该机器的哪些知识呢？

名称编号类型的使用：

00 U 工作站服务

01 U 邮件服务

\\_M 好好学习 ROWSE\_ 01 G 主浏览器

03 U 邮件服务

06 U RAS 服务器服务

1F U NetDDE 服务

20 U 文件服务器服务

21 U RAS 客户机服务

22 U Exchange Interchange

23 U Exchange Store

24 U Exchange Directory

30 U 调制解调器共享服务器服务

31 U 调制解调器共享客户机服务

43 U SMS 客户机远程控制

44 U SMS 管理远程控制工具

45 U SMS 客户机远程聊天

46 U SMS 客户机远程传输

4C U DEC Pathworks TCP/IP 服务

52 U DEC Pathworks TCP/IP 服务

87 U Exchange MTA

6A U Exchange IMC

BE U 网络监控代理

BF U 网络监控应用

03 U 邮件服务

00 G 域名

1B U 域主浏览器

1C G 域控制器

1D U 主浏览器

1E G 浏览器服务选择

1C G Internet 信息服务器

00 U Internet 信息服务器

[2B] U Lotus Notes 服务器

IRISMULTICAST [2F] G Lotus Notes

IRISNAMESERVER [33] G Lotus Notes

Forte\_\$ND800ZA [20] U DCA Irmalan 网关服务

Unique (U): 该名字可能只有一个分配给它的 IP 地址。在网络设备上，一个要注册的名字

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 地址等。在此我们就有必要了解几个基本的参数。

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

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

-n 列出本地机器的 NETBIOS 信息。

当得到了对方的 IP 或者机器名的时候，就可以使用 nbtstat 命令来进一步得到对方的信息了，这又增加了我们入侵的保险系数。

### 三、netstat

Netstat 用于显示与 IP、TCP、UDP 和 ICMP 协议相关的统计数据，一般用于检验本机各端口的网络连接情况。

如果你的计算机有时候接收到的数据报导致出错数据或故障，你不必感到奇怪，TCP/IP 可以容许这些类型的错误，并能够自动重发数据报。但如果累计的出错情况数目占到所接收的 IP 数据报相当大的百分比，或者它的数目正迅速增加，那么你就应该使用 Netstat 查一查为什么会出现这些情况了。

Netstat 详细参数列表

(Winxp)

C:\>netstat /?

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\zykun>netstat /?

显示协议统计信息和当前 TCP/IP 网络连接。

NETSTAT [-a] [-b] [-e] [-n] [-o] [-p proto] [-r] [-s] [-v] [interval]

-a          显示所有连接和监听端口。
-b          显示包含于创建每个连接或监听端口的可执行组件。在某些情况下已知可执行组件拥有多个独立组件，并且在这些情况下包含于创建连接或监听端口的组件序列被显示。这种情况下，可执行组件名在底部的 [] 中，顶部是其调用的组件，等等，直到 TCP/IP 部分。注意此选项可能需要很长时间，如果没有足够权限可能失败。
-e          显示以太网统计信息。此选项可以与 -s 选项组合使用。
-n          以数字形式显示地址和端口号。
-o          显示与每个连接相关的所属进程 ID。
-p proto    显示 proto 指定的协议的连接；proto 可以是下列协议之一：TCP、UDP、TCPv6 或 UDPv6。
            如果与 -s 选项一起使用以显示按协议统计信息，proto 可以是下列协议之一：
            IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP 或 UDPv6。
-r          显示路由表。
-s          显示按协议统计信息。默认地，显示 IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP 和 UDPv6 的统计信息；-p 选项用于指定默认情况的子集。
-v          与 -b 选项一起使用时将显示包含于为所有可执行组件创建连接或监听端口的组件。
interval    重新显示选定统计信息，每次显示之间暂停时间间隔<以秒计>。按 CTRL+C 停止重新显示统计信息。如果省略，netstat 显示当前配置信息<只显示一次>
```

显示协议统计信息和当前 TCP/IP 网络连接。

NETSTAT [-a] [-b] [-e] [-n] [-o] [-p proto] [-r] [-s] [-v] [interval]

- a 以机器名字显示所有连接和监听端口。
- n 以数字形式显示地址和端口号。
- b 显示包含于创建每个连接或监听端口的可执行组件。在某些情况下已知可执行组件拥有多个独立组件，并且在这些情况下包含于创建连接或监听端口的组件序列被显示。这种情况下，可执行组件名在底部的 [] 中，顶部是其调用的组件，等等，直到 TCP/IP 部分。注意此选项可能需要很长时间，如果没有足够权限可能失败。
- e 显示以太网统计信息。此选项可以与 -s 选项组合使用。
- o 显示与每个连接相关的所属进程 ID。
- p proto 显示 proto 指定的协议的连接；proto 可以是下列协议之一：TCP、UDP、TCPv6 或 UDPv6。如果与 -s 选项一起使用以显示按协议统计信息，proto 可以是下列协议之一：IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP 或 UDPv6。

**-r** 显示路由表。（和 **route print** 命令相同的功能）

**-s** 显示按协议统计信息。默认地，显示 IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP 和 UDPv6 的统计信息；

**-p** 选项用于指定默认情况的子集。

**-v** 与 **-b** 选项一起使用时将显示包含于为所有可执行组件创建连接或监听端口的组件。

**interval** 重新显示选定统计信息，每次显示之间暂停时间间隔(以秒计)。按 CTRL+C 停止重新显示统计信息。如果省略，**netstat** 显示当前配置信息(只显示一次)

### (Win2000)

C:\>netstat /?

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-e] [-n] [-s] [-p proto] [-r] [interval]

**-a** Displays all connections and listening ports.

**-e** Displays Ethernet statistics. This may be combined with the **-s** option.

**-n** Displays addresses and port numbers in numerical form.

**-p proto** Shows connections for the protocol specified by proto; proto may be TCP or UDP. If used with the **-s** option to display per-protocol statistics, proto may be TCP, UDP, or IP.

**-r** Displays the routing table.

**-s** Displays per-protocol statistics. By default, statistics are shown for TCP, UDP and IP; the **-p** option may be used to specify a subset of the default.

**interval** Redisplays selected statistics, pausing interval seconds between each display. Press CTRL+C to stop redisplaying statistics. If omitted, netstat will print the current configuration information once.

### Netstat 的一些常用选项

**netstat -s**——本选项能够按照各个协议分别显示其统计数据。如果你的应用程序（如 Web 浏览器）运行速度比较慢，或者不能显示 Web 页之类的数据，那么你就可以用本选项来查看一下所显

示的信息。你需要仔细查看统计数据的各行，找到出错的关键字，进而确定问题所在。

**netstat -e**——本选项用于显示关于以太网的统计数据。它列出的项目包括传送的数据报的总字节数、错误数、删除数、数据报的数量和广播的数量。这些统计数据既有发送的数据报数量，也有接收的数据报数量。这个选项可以用来统计一些基本的网络流量。

**netstat -r**——本选项可以显示关于路由表的信息，类似于后面所讲使用 route print 命令时看到的信息。除了显示有效路由外，还显示当前有效的连接。

**netstat -a**——本选项显示一个所有的有效连接信息列表，包括已**建立的连接（ESTABLISHED）**，也包括**监听连接请求（LISTENING）**的那些连接，**断开连接（CLOSE\_WAIT）**或者处于**联机等待状态的（TIME\_WAIT）**等

(ESTABLISHED)    建立的连接  
(LISTENING)      监听连接请求  
(CLOSE\_WAIT)    断开连接  
(TIME\_WAIT)     联机等待

**netstat -n**——显示所有已建立的有效连接。

微软公司故意将这个功能强大的命令隐藏起来是因为它对于普通用户来说有些复杂。我们已经知道：Netstat 它可以用来获得你的系统网络连接的信息（使用的端口，在使用的协议等），收到和发出的数据，被连接的远程系统的端口，Netstat 在内存中读取所有的网络信息。

在 Internet RFC 标准中，Netstat 的定义是：Netstat 是在内核中访问网络及相关信息的程序，它能提供 TCP 连接，TCP 和 UDP 监听，进程内存管理的相关报告。

对于好奇心极强的人来说，紧紧有上面的理论是远远不够的，接下来我们来详细的解释一下各个参数的使用，看看执行之后会发生什么，显示的信息又是什么意思，好了，废话不说了，让我们一起来实践一下吧：)

```
C:\>netstat -a
```

Active Connections

	Proto	Local Address	Foreign Address	State
	TCP	Eagle:ftp	Eagle:	
0				LISTENING
	TCP	Eagle:telnet	Eagle:	
0				LISTENING
	TCP	Eagle:smtp	Eagle:	
0				LISTENING
	TCP	Eagle:http	Eagle:	
0				LISTENING
	TCP	Eagle:epmap	Eagle:	
0				LISTENING
	TCP	Eagle:https	Eagle:	



0		LISTENING		
	TCP	Eagle:microsoft-ds	Eagle:0	LISTENING
	TCP	Eagle:1030	Eagle:	
0		LISTENING		
	TCP	Eagle:6059	Eagle:	
0		LISTENING		
	TCP	Eagle:8001	Eagle:	
0		LISTENING		
	TCP	Eagle:8005	Eagle:	
0		LISTENING		
	TCP	Eagle:8065	Eagle:	
0		LISTENING		
	TCP	Eagle:microsoft-ds	localhost:1031	ESTABLISHED
	TCP	Eagle:1031	localhost:microsoft-ds	ESTABLISHED
	TCP	Eagle:1040	Eagle:	
0		LISTENING		
	TCP	Eagle:netbios-ssn	Eagle:0	LISTENING
	TCP	Eagle:1213	218.85.139.65:9002	CLOSE_WAIT
	TCP	Eagle:2416	219.133.63.142:https	CLOSE_WAIT
	TCP	Eagle:2443	219.133.63.142:https	CLOSE_WAIT
	TCP	Eagle:2907	192.168.1.101:2774	CLOSE_WAIT
	TCP	Eagle:2916	192.168.1.101:telnet	ESTABLISHED
	TCP	Eagle:2927	219.137.227.10:4899	TIME_WAIT
	TCP	Eagle:2928	219.137.227.10:4899	TIME_WAIT
	TCP	Eagle:2929	219.137.227.10:4899	ESTABLISHED
	TCP	Eagle:3455	218.85.139.65:9002	ESTABLISHED
	TCP	Eagle:netbios-ssn	Eagle:0	LISTENING
	UDP	Eagle:microsoft-ds	*:*	
	UDP	Eagle:1046	*:*	
	UDP	Eagle:1050	*:*	
	UDP	Eagle:1073	*:*	
	UDP	Eagle:1938	*:*	
	UDP	Eagle:2314	*:*	

UDP	Eagle:2399		*:*
UDP	Eagle:2413		*:*
UDP	Eagle:2904		*:*
UDP	Eagle:2908		*:*
UDP	Eagle:3456		*:*
UDP	Eagle:4000		*:*
UDP	Eagle:4001		*:*
UDP	Eagle:6000		*:*
UDP	Eagle:6001		*:*
UDP	Eagle:6002		*:*
UDP	Eagle:6003		*:*
UDP	Eagle:6004		*:*
UDP	Eagle:6005		*:*
UDP	Eagle:6006		*:*
UDP	Eagle:6007		*:*
UDP	Eagle:6008		*:*
UDP	Eagle:6009		*:*
UDP	Eagle:6010		*:*
UDP	Eagle:6011		*:*
UDP	Eagle:1045		*:*
UDP	Eagle:1051		*:*
UDP	Eagle:netbios-ns	*:*	
UDP	Eagle:netbios-dgm	*:*	
UDP	Eagle:netbios-ns	*:*	
UDP	Eagle:netbios-dgm	*:*	

我们拿其中一行来解释吧：

Proto	Local Address	Foreign Address	State
TCP	Eagle:2929	219.137.227.10:4899	ESTABLISHED

协议（Proto）：TCP，指的是传输层通讯协议（什么？不懂？请用 baidu 搜索“TCP”，OSI 七层和 TCP/IP 四层可是基础^\_^）

本地机器名（Local Address）：Eagle，俗称计算机名了，安装系统时设置的，可以在“我的电脑”属性中修改，本地打开并用于连接的端口：2929）

远程机器名（Foreign Address）：219.137.227.10

远程端口：4899

状态：ESTABLISHED

## 状态列表

LISTEN：在监听状态中。

ESTABLISHED：已建立联机的联机情况。

TIME\_WAIT：该联机在目前已经是等待的状态。

-a 参数常用于获得你的本地系统开放的端口，用它您可以自己检查你的系统上有没有被安装木马（ps：有很多好程序用来检测木马，但你的目的是想成为真正的 hacker，手工检测要比只按一下“scan”按钮好些——仅个人观点）。如果您 Netstat 你自己的话，发现下面的信息：

```
Port 12345(TCP) Netbus
Port 31337(UDP) Back Orifice
```

祝贺！您中了最常见的木马（^\_^，上面 4899 是我连别人的，而且这个 radmin 是商业软件，目前我最喜欢的远程控制软件）

如果你需要木马及其端口列表的话，去国内的 H 站找找，或者 baidu，google 吧

\*\*\*\*\*

#一些原理：也许你有这样的问题：“在机器名后的端口号代表什么？”

例子：Eagle:2929

小于 1024 的端口通常运行一些网络服务，大于 1024 的端口用来与远程机器建立连接。

\*\*\*\*\*

继续我们的探讨，使用 -n 参数。（Netstat -n）

Netstat -n 基本上是 -a 参数的数字形式：

```
C:\>netstat -n
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:445	127.0.0.1:1031	ESTABLISHED
SHED			
TCP	127.0.0.1:1031	127.0.0.1:445	ESTABLISHED
SHED			
TCP	192.168.1.180:1213	218.85.139.65:9002	CLOSE_WAIT
TCP	192.168.1.180:2416	219.133.63.142:443	CLOSE_WAIT
TCP	192.168.1.180:2443	219.133.63.142:443	CLOSE_WAIT
TCP	192.168.1.180:2907	192.168.1.101:2774	CLOSE_WAIT
TCP	192.168.1.180:2916	192.168.1.101:23	ESTABLISHED
TCP	192.168.1.180:2929	219.137.227.10:4899	ESTABLISHED
TCP	192.168.1.180:3048	192.168.1.1:8004	SYN_SENT
TCP	192.168.1.180:3455	218.85.139.65:9002	ESTABLISHED

netstat -an 这个命令能看到所有和本地计算机建立连接的 IP，它包含四个部分——proto（连接方式）、local address（本地连接地址）、foreign address（和本地建立连接的地址）、state（当前端口状态）。

-a 和 -n 是最常用的两个，据我不完全测试得出以下结果：

1. -n 显示用数字化主机名，即 IP 地址，而不是 compute\_name【eagle】

2. -n 只显示 TCP 连接（没有在哪里见过微软的相关文档，有哪个朋友见到的话，记得告诉我喔^\_^）

得到 IP 等于得到一切，它是最容易使机器受到攻击的东东，所以隐藏自己 IP，获得别人的 IP 对 hacker 来说非常重要，现在隐藏 IP 技术很流行，但那些隐藏工具或服务真的让你隐身吗？我看不见得，呵呵，代理，跳板不属于今天讨论，一个获取对方 IP 的简单例子请参考我前面的文章【[用 DOS 命令查 QQ 好友 IP 地址](#)】

-a 和 -n 是最常用的命令，如果要显示一些协议的更详细信息，就要用 -p 这个参数了，它其实是 -a 和 -n 的一个变种，我们来看一个实例，你就明白了：【netstat -p @@@ 其中 @@@ 为 TCP 或者 UDP】

```
C:\>netstat -p tcp
```

Active Connections

	Proto	Local Address	Foreign Address	State
	TCP	Eagle:microsoft-ds	localhost:1031	ESTABLISHED
	TCP	Eagle:1031	localhost:microsoft-ds	ESTABLISHED
D				
	TCP	Eagle:1213	218.85.139.65:9002	CLOSE_WAIT
IT				
	TCP	Eagle:2416	219.133.63.142:https	CLOSE_WAIT
	TCP	Eagle:2443	219.133.63.142:https	CLOSE_WAIT
	TCP	Eagle:2907	192.168.1.101:2774	CLOSE_WAIT
IT				
	TCP	Eagle:2916	192.168.1.101:telnet	ESTABLISHED
D				
	TCP	Eagle:2929	219.137.227.10:4899	ESTABLISHED
ED				
	TCP	Eagle:3455	218.85.139.65:9002	ESTABLISHED
HED				

继续我们的参数讲解 -e

含义：本选项用于显示关于以太网的统计数据。它列出的项目包括传送的数据报的总字节数、错误数、删除数、数据报的数量和广播的数量。这些统计数据既有发送的数据报数量，也有接收的数据报数量。这个选项可以用来统计一些基本的网络流量。

```
C:\>netstat -e
```

Interface Statistics

	Receive	
	Sent	
d		
Bytes	143090206	44998789
Unicast packets	691805	363603
Non-unicast packets	886526	2386
Discards		
0	0	

Errors

0 0

Unknown protocols 4449

若接收错和发送错接近为零或全为零，网络的接口无问题。但当这两个字段有 100 个以上的出错分组时就可以认为是高出错率了。高的发送错表示本地网络饱和或在主机与网络之间有不良的物理连接；高的接收错表示整体网络饱和、本地主机过载或物理连接有问题，可以用 Ping 命令统计误码率，进一步确定故障的程度。netstat -e 和 ping 结合使用能解决一大部分网络故障。

接下来我们开始讲解两个比较复杂的参数 -r 和 -s，也正因为如此，笔者把他放到最后讲解，这里面可能会涉及到其他方面的知识，以后在我的博客中将会继续写出来，呵呵，最近比较忙

-r 是用来显示路由表信息，我们来看例子：

C:\>netstat -r

Route Table (路由表)

=====

Interface List (网络接口列表)

0x1 ..... MS TCP Loopback interface

0x10003 ...00 0c f1 02 76 81 ..... Intel(R) PRO/Wireless LAN 2100 3B Mini PCI  
dapter

0x10004 ...00 02 3f 00 05 cb ..... Realtek RTL8139/810x Family Fast Ethernet  
C

=====

=====

Active Routes: (动态路由)

Network Interface	Destination Metric	Netmask	Gateway	Int erface
	0.0.0.0	0.0.0.0	192.168.1.254	192.16
8.1.181	30			
	0.0.0.0	0.0.0.0	192.168.1.254	192.16
8.1.180	20			
	127.0.0.0	255.0.0.0	127.0.0.	
1	127.0.0.1	1		
	192.168.1.0	255.255.255.0	192.168.1.180	192.168.1.18
0	20			
	192.168.1.0	255.255.255.0	192.168.1.181	192.168.1.18
1	30			
	192.168.1.180	255.255.255.255	127.0.0.1	127.0.0.
1	20			
	192.168.1.181	255.255.255.255	127.0.0.1	127.0.0.
1	30			

```

0          192.168.1.255    255.255.255.255          192.168.1.180    192.168.1.18
          20
1          192.168.1.255    255.255.255.255          192.168.1.181    192.168.1.18
          30
          224.0.0.0          240.0.0.0          192.168.1.180    192.168.1.
180          20
          224.0.0.0          240.0.0.0          192.168.1.181    192.168.1.
181          30
          255.255.255.255    255.255.255.255          192.168.1.180    192.168.1.18
0          1
          255.255.255.255    255.255.255.255          192.168.1.181    192.168.1.18
1          1
Default Gateway:          192.168.1.254 (默认网关)
=====
Persistent Routes: (静态路由)
    None
C:\>

```

**-s** 参数的作用前面有详细的说明，来看例子

C:\>netstat -s

IPv4 Statistics

(IP 统计结果)

Packets Received	= 369492 (接收包数)
Received Header Errors	= 0 (接收头错误数)
Received Address Errors	= 2 (接收地址错误数)
Datagrams Forwarded	= 0 (数据报递送数)
Unknown Protocols Received	= 0 (未知协议接收数)
Received Packets Discarded	= 4203 (接收后丢弃的包数)
Received Packets Delivered	= 365287 (接收后转交的包数)
Output Requests	= 369066 (请求数)
Routing Discards	= 0 (路由丢弃数)
Discarded Output Packets	= 2172 (包丢弃数)
Output Packet No Route	= 0 (不路由的请求包)
Reassembly Required	= 0 (重组的请求数)
Reassembly Successful	= 0 (重组成功数)
Reassembly Failures	= 0 (重组失败数)
Datagrams Successfully Fragmented	= 0 (分片成功的数据报数)
Datagrams Failing Fragmentation	= 0 (分片失败的数据报数)
Fragments Created	= 0 (分片建立数)

ICMPv4 Statistics (ICMP 统计结果) 包括 Received 和 Sent 两种状态

	Received	Sent
Messages	285	784 (消息数)
Errors	0	0 (错误数)

```

Destination Unreachable      53              548（无法到达主机数目）
Time Exceeded                 0              0（超时数目）
Parameter Problems           0              0（参数错误）
Source Quenches               0              0（源夭折数）
Redirects                     0              0（重定向数）
Echos                        25              211（回应数）
Echo Replies                  207            25（回复回应数）
Timestamps                    0              0（时间戳数）
Timestamp Replies             0              0（时间戳回复数）
Address Masks                 0              0（地址掩码数）
Address Mask Replies          0              0（地址掩码回复数）
TCP Statistics for IPv4（TCP 统计结果）
Active Opens                  = 5217（主动打开数）
Passive Opens                  = 80（被动打开数）
Failed Connection Attempts    = 2944（连接失败尝试数）
Reset Connections              = 529（复位连接数）
Current Connections           = 9（当前连接数目）
Segments Received              = 350143（当前已接收的报文
数）
Segments Sent                  = 347561（当前已发送的
报文数）
Segments Retransmitted        = 6108（被重传的报文数目）
UDP Statistics for IPv4（UDP 统计结果）
Datagrams Received            = 14309（接收的数据包）
No Ports                       = 1360（无端口数）
Receive Errors                 = 0（接收错误数）
Datagrams Sent                 = 14524（数据包发送数）
C:\>

```

## 四、tracert

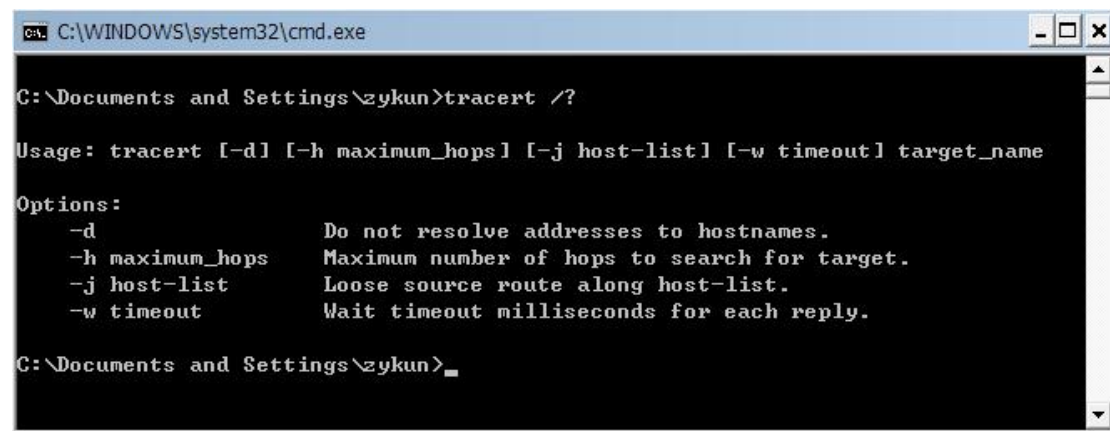
Tracert（跟踪路由）是路由跟踪实用程序，用于确定 IP 数据报访问目标所采取的路径。

该命令用 IP 生存时间（TTL）字段和 ICMP 错误消息来确定从一个主机到网络上其他主机的路由。

### Tracert 工作原理

通过向目标发送不同 IP 生存时间（TTL）值的“Internet 控制消息协议（ICMP）”回应数据包，Tracert 诊断程序确定到目标所采取的路由。要求路径上

的每个路由器在转发数据包之前至少将数据包上的 TTL 递减 1。数据包上的 TTL 减为 0 时，路由器应该将“ICMP 已超时”的消息发回源系统。



```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\zykun>tracert /?

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name

Options:
    -d                Do not resolve addresses to hostnames.
    -h maximum_hops   Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list.
    -w timeout         Wait timeout milliseconds for each reply.

C:\Documents and Settings\zykun>
```

Tracert 先发送 TTL 为 1 的回应数据包，并在随后的每次发送过程将 TTL 递增 1，直到目标响应或 TTL 达到最大值，从而确定路由。通过检查中间路由器发回的“ICMP 已超时”的消息确定路由。某些路由器不经询问直接丢弃 TTL 过期的数据包，这在 Tracert 实用程序中看不到。

Tracert 命令按顺序打印出返回“ICMP 已超时”消息的路径中的近端路由器接口列表。如果使用 -d 选项，则 Tracert 实用程序不在每个 IP 地址上查询 DNS。

**例：**

数据包必须通过两个路由器（10.0.0.1 和 192.168.0.1）才能到达主机 172.16.0.99。

主机的默认网关是 10.0.0.1，192.168.0.0 网络上的路由器的 IP 地址是 192.168.0.1。

```
C:\>tracert 172.16.0.99 -d
```

```
Tracing route to 172.16.0.99 over a maximum of 30 hops
```

```
1 2s 3s 2s 10,0.0,1
```

```
2 75 ms 83 ms 88 ms 192.168.0.1
```

```
3 73 ms 79 ms 93 ms 172.16.0.99
```

```
Trace complete.
```

用 tracert 解决问题



可以使用 `tracert` 命令确定数据包在网络上的停止位置。

例：

默认网关确定 192.168.10.99 主机没有有效路径。这可能是路由器配置的问题，或者是 192.168.10.0 网络不存在（错误的 IP 地址）。

```
C:\>tracert 192.168.10.99
```

```
Tracing route to 192.168.10.99 over a maximum of 30 hops
```

```
  1  10.0.0.1 reports:Destination net unreachable.
```

```
Trace complete.
```

Tracert 实用程序对于解决大网络问题非常有用，此时可以采取几条路径到达同一个点。

Tracert 命令行选项

Tracert 命令支持多种选项，如下表所示。

```
tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]  
target_name
```

**-d**

指定不将 IP 地址解析到主机名称。

**-h maximum\_hops**

指定跃点数以跟踪到称为 `target_name` 的主机的路由。

**-j host-list**

指定 Tracert 实用程序数据包所采用路径中的路由器接口列表。

**-w timeout**

等待 `timeout` 为每次回复所指定的毫秒数。

**target\_name**

目标主机的名称或 IP 地址。

## 五、net

这个命令是网络命令中最重要的一個，必須透徹掌握它的每一個子命令的用法，因为它

的功能实在是太强大了，这简直就是 微软为我们提供的最好的入侵工具。首先让我们来看一看它都有那些子命令，键入 `net /?`回车。

在这里，我们重点掌握几个入侵常用的子命令。

#### `net view`

使用此命令查看远程主机的所以共享资源。命令格式为 `net view IP`。

#### `net use`

把远程主机的某个共享资源影射为本地盘符，图形界面方便使用，呵呵。命令格式为 `net use x: IPsharename`。上面一个表示把 192.168.0.5IP 的共享名为 magic 的目录影射为本地的 Z 盘。下面表示和 192.168.0.7 建立 IPC\$连接（`net use IP IPC$"password" /user:"name"`）。

建立了 IPC\$连接后，呵呵，就可以上传文件了：`copy nc.exe 92.168.0.7admin$`，表示把本地目录下的 nc.exe 传到远程主机，结合后面要介绍到的其他 DOS 命令就可以实现入侵了。

#### `net start`

使用它来启动远程主机上的服务。当你和远程主机建立连接后，如果发现它的什么服务没有启动，而你又想利用此服务怎么办？就使用这个命令来启动吧。用法：`net start server name`，成功启动了 telnet 服务。

#### `net stop`

入侵后发现远程主机的某个服务碍手碍脚，怎么办？利用这个命令停掉就 ok 了，用法和 `net start` 同。

#### `net user`

查看和帐户有关的情况，包括新建帐户、删除帐户、查看特定帐户、激活帐户、帐户禁用等。这对我们入侵是很有利的，最重要的，它为我们克隆帐户提供了前提。键入不带参数的 `net user`，可以查看所有用户，包括已经禁用的。下面分别讲解。

1, `net user abcd 1234 /add`，新建一个用户名为 abcd，密码为 1234 的帐户，默认为 user 组成员。

2, `net user abcd /del`，将用户名为 abcd 的用户删除。

3, `net user abcd /active:no`, 将用户名为 `abcd` 的用户禁用。

4, `net user abcd /active:yes`, 激活用户名为 `abcd` 的用户。

5, `net user abcd`, 查看用户名为 `abcd` 的用户的情况。

#### `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帐户提升为 `administrator` 组帐户, 这样我们利用这个帐户 就可以控制整个远程主机了。用法: `net localgroup groupname username /add`。

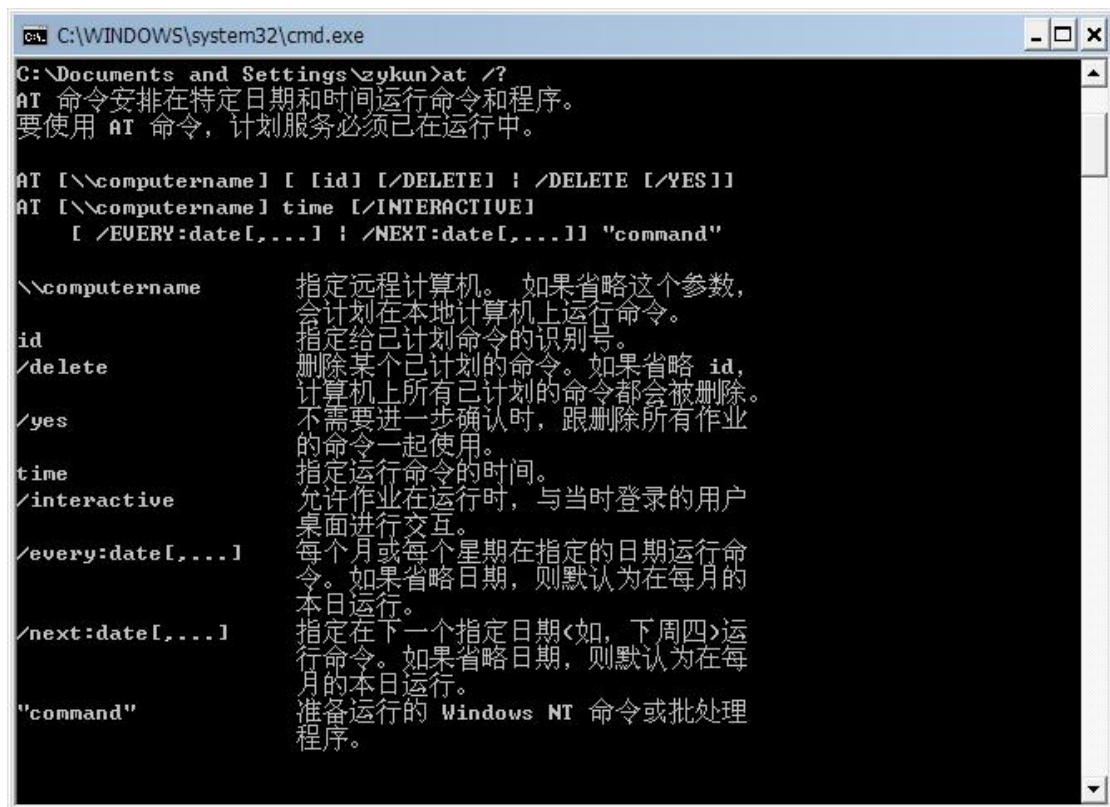
现在我们把刚才新建的用户 `abcd` 加到 `administrator` 组里去了, 这时候 `abcd` 用户已经是超级管理员了, 呵呵, 你可以再使用 `net user abcd` 来查看他的状态。但这样太明显了, 网管一看用户情况就能漏出破绽, 所以这种方法只能对付菜鸟网管, 但我们还得知。现在的手段都是利用其他工具和 手段克隆一个让网管看不出来的超级管理员, 这是后话。有兴趣的朋友可以参照《黑客防线》第 30 期上的《由浅入深解析隆帐户》一文。

#### `net time`

这个命令可以查看远程主机当前的时间。如果你的目标只是进入到远程主机里面, 那么也许就用不到这个命令了。但简单的入侵成功了, 难道只是看看吗? 我们 需要进一步渗透。这就连远程主机当前的时间都需要知道, 因为利用时间和其他手段(后面会讲到)可以实现某个命令和程序的定时启动, 为我们进一步入侵打好基础。用法: `net time IP`。

## 六、at

这个命令的作用是安排在特定日期或时间执行某个特定的命令和程序(知道 `net time` 的重要了吧? )。当我们知道了远程主机的当前时间, 就可以利用此命令让其在以后的某个时间(比如 2 分钟后)执行某个程序和命令。用法: `at time command computer`。



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\zykun>at /?
AT 命令安排在特定日期和时间运行命令和程序。
要使用 AT 命令，计划服务必须已在运行中。

AT [[\computername] [ [id] [/DELETE] : /DELETE [/YES]]
AT [[\computername] time [/INTERACTIVE]
    [ /EVERY:date[,...]] : /NEXT:date[,...]] "command"

\\computername    指定远程计算机。 如果省略这个参数，
                  会计划在本地计算机上运行命令。
id                指定给已计划命令的识别号。
/delete           删除某个已计划的命令。如果省略 id，
                  计算机上所有已计划的命令都会被删除。
/yes              不需要进一步确认时，跟删除所有作业的
                  命令一起使用。
time              指定运行命令的时间。
/interactive      允许作业在运行时，与当时登录的用户
                  桌面进行交互。
/every:date[,...] 每个月或每个星期在指定的日期运行命
                  令。如果省略日期，则默认为在每月的
                  本日运行。
/next:date[,...]  指定在下一个指定日期(如，下周四)运
                  行命令。如果省略日期，则默认为在每
                  月的本日运行。
"command"         准备运行的 Windows NT 命令或批处理
                  程序。
```

表示在 6 点 55 分时，让名称为 a-01 的计算机开启 telnet 服务（这里 net start telnet 即为开启 telnet 服务的命令）。

## 七、ftp

大家对这个命令应该比较熟悉了吧？网络上开放的 ftp 的主机很多，其中很大一部分是匿名的，也就是说任何人都可以登陆上去。现在如果你扫到了一台开放 ftp 服务的主机（一般都是开了 21 端口的机器），如果你还不会使用 ftp 的命令怎么办？下面就给出基本的 ftp 命令使用方法。

首先在命令行键入 ftp 回车，出现 ftp 的提示符，这时候可以键入"help"来查看帮助（任何 DOS 命令都可以使用此方法查看其帮助）。

大家可能看到了，这么多命令该怎么用？其实也用不到那么多，掌握几个基本的就够了。

首先是登陆过程，这就要用到 open 了，直接在 ftp 的提示符下输入"open 主机 IP ftp 端口"回车即可，一般端口默认都是 21，可以不写。接着就是输入合法的用户名和密码进行登陆了，这里以匿名 ftp 为例介绍。

用户名和密码都是 ftp，密码是不显示的。当提示\*\*\*\* logged in 时，就说明登陆成功。

这里因为是匿名登陆，所以用户显示为 **Anonymous**。

接下来就要介绍具体命令的使用方法了。

**dir** 跟 DOS 命令一样，用于查看服务器的文件，直接敲上 **dir** 回车，就可以看到此 **ftp** 服务器上的文件。

**cd** 进入某个文件夹。

**get** 下载文件到本地机器。

**put** 上传文件到远程服务器。这就要看远程 **ftp** 服务器是否给了你可写的权限了，如果可以，呵呵，该怎么 利用就不多说了，大家就自由发挥去吧。

**delete** 删除远程 **ftp** 服务器上的文件。这也必须保证你有可写的权限。

**bye** 退出当前连接。

**quit** 同上。

## 八、telnet

功能强大的远程登陆命令，几乎所有的入侵者都喜欢用它，屡试不爽。为什么？它操作简单，如同使用自己的机器一样，只要你熟悉 DOS 命令，在成功以 **administrator** 身份连接了远程机器后，就可以用它来\*想干的一切了。下面介绍一下使用方法，首先键入 **telnet** 回车，再键入 **help** 查看其 帮助信息。



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\zykun>telnet /?

telnet [-a][-e escape char][-f log file][-l user][-t term][host [port]]
-a      企图自动登录。除了用当前已登陆的用户名以外，与 -l 选项相同。
-e      跳过字符来进入 telnet 客户提示。
-f      客户端登录的文件名
-l      指定远程系统上登录用的用户名称。
        要求远程系统支持 TELNET ENVIRON 选项。
-t      指定终端类型。
        支持的终端类型仅是: vt100, vt52, ansi 和 vtnt。
host    指定要连接的远程计算机的主机名或 IP 地址。
port    指定端口号或服务名。

C:\Documents and Settings\zykun>
```

然后在提示符下键入 **open IP** 回车，这时就出现了登陆窗口，让你输入合法的用户名和密码，这里输入任何密码都是不显示的。

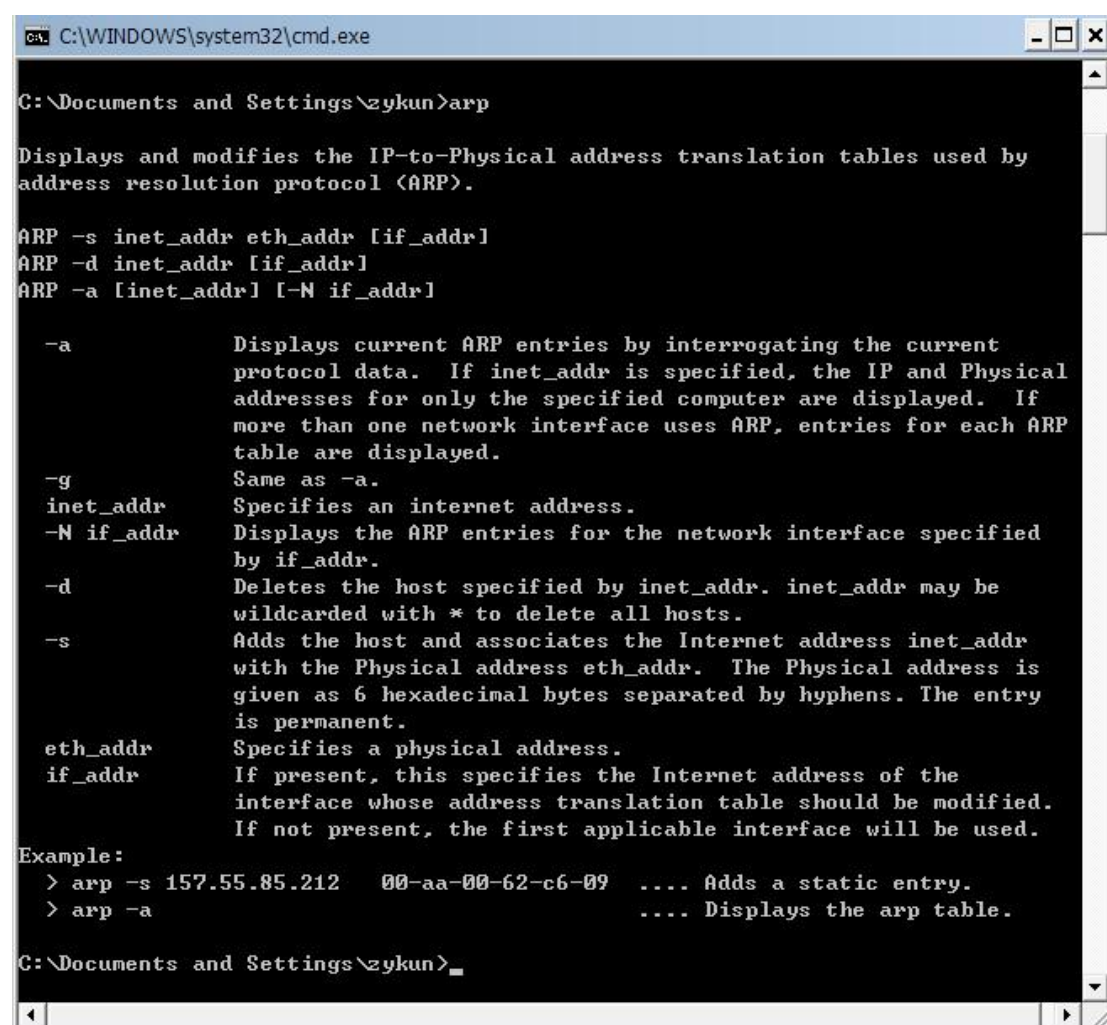
当输入用户名和密码都正确后就成功建立了 **telnet** 连接，这时候你就在远程主机上具有了和此用户一样的权限，利用 DOS 命令就可以实现你想干的事情了。这里我使用的超级管理员权限登陆的。

到这里为止，网络 DOS 命令的介绍就告一段落了，这里介绍的目的只是给菜鸟网管一个印象，让其知道熟悉和掌握网络 DOS 命令的重要性。其实和网络有关的 DOS 命令还远不止这些，这里只是抛砖引玉，希望能对广大菜鸟网管有所帮助。学好 DOS 对当好网管有很大的帮助，特别的熟练掌握了一些网络的 DOS 命令。

另外大家应该清楚，任何人要想进入系统，必须得有一个合法的用户名和密码（输入法漏洞差不多绝迹了吧），哪怕你拿到帐户的只有一个很小的权限，你也可以利用它来达到最后的目的。所以坚决消灭空口令，给自己的帐户加上一个强壮的密码，是最好的防御弱口令入侵的方法。

## 九、ARP

ARP 是一个重要的 TCP/IP 协议，并且用于确定对应 IP 地址的网卡物理地址。实用 arp 命令，我们能够查看本地计算机或另一台计算机的 ARP 高速缓存中的当前内容。此外，使用 arp 命令，也可以用人工方式输入静态的网卡物理/IP 地址对，我们可能会使用这种方式为缺省网关和本地服务器等常用主机进行这项作，有助于减少网络上的信息量。



```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\zykun>arp

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr]

-a          Displays current ARP entries by interrogating the current
            protocol data. If inet_addr is specified, the IP and Physical
            addresses for only the specified computer are displayed. If
            more than one network interface uses ARP, entries for each ARP
            table are displayed.
-g          Same as -a.
inet_addr   Specifies an internet address.
-N if_addr  Displays the ARP entries for the network interface specified
            by if_addr.
-d          Deletes the host specified by inet_addr. inet_addr may be
            wildcarded with * to delete all hosts.
-s          Adds the host and associates the Internet address inet_addr
            with the Physical address eth_addr. The Physical address is
            given as 6 hexadecimal bytes separated by hyphens. The entry
            is permanent.
eth_addr    Specifies a physical address.
if_addr     If present, this specifies the Internet address of the
            interface whose address translation table should be modified.
            If not present, the first applicable interface will be used.

Example:
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Adds a static entry.
> arp -a                                     .... Displays the arp table.

C:\Documents and Settings\zykun>
```

按照缺省设置，ARP 高速缓存中的项目是动态的，每当发送一个指定地点的数据报且高速缓存中不存在当前项目时，ARP 便会自动添加该项目。一旦高速缓存的项目被输入，它们就已经开始走向失效状态。例如，在 Windows NT/2000 网络中，如果输入项目后不进一步使用，

物理/IP 地址对就会在 2 至 10 分钟内失效。因此，如果 ARP 高速缓存中项目很少或根本没有时，请不要奇怪，通过另一台计算机或路由器的 ping 命令即可添加。所以，需要通过 arp 命令查看高速缓存中的内容时，请最好先 ping 此台计算机（不能是本机发送 ping 命令）。

ARP 常用命令选项：

·arp -a 或 arp -g

用于查看高速缓存中的所有项目。-a 和-g 参数的结果是一样的，多年来-g 一直是 UNIX 平台上用来显示 ARP 高速缓存中所有项目的选项，而 Windows 用的是 arp -a（-a 可被视为 all，即全部的意思），但它也可以接受比较传统的-g 选项。

·arp -a IP

如果我们有多个网卡，那么使用 arp -a 加上接口的 IP 地址，就可以只显示与该接口相关的 ARP 缓存项目。

·arp -s IP 物理地址

我们可以向 ARP 高速缓存中人工输入一个静态项目。该项目在计算机引导过程中将保持有效状态，或者在出现错误时，人工配置的物理地址将自动更新该项目。

·arp -d IP

使用本命令能够人工删除一个静态项目。

例如我们在命令提示符下，键入 Arp -a；如果我们使用过 Ping 命令测试并验证从这台计算机到 IP 地址为 10.0.0.99 的主机的连通性，则 ARP 缓存显示以下项：

Interface:10.0.0.1 on interface 0x1

Internet Address	Physical Address	Type
10.0.0.99	00-e0-98-00-7c-dc	dynamic

在此例中，缓存项指出位于 10.0.0.99 的远程主机解析成 00-e0-98-00-7c-dc 的媒体访问控制地址，它是在远程计算机的网卡硬件中分配的。媒体访问控制地址是计算机用于与网络上远程 TCP/IP 主机物理通讯的地址。

至此我们可以用 ipconfig 和 ping 命令来查看自己的网络配置并判断是否正确、可以用 ne



**tstat** 查看别人与我们所建立连接并找出 **ICQ** 使用者所隐藏的 **IP** 信息、可以用 **arp** 查看网卡的 **MAC** 地址。

## Tracert

如果有网络连通性问题，可以使用 **tracert** 命令来检查到达的目标 **IP** 地址的路径并记录结果。**tracert** 命令显示用于将数据包从计算机传递到目标位置的一组 **IP** 路由器，以及每个跃点所需的时间。如果数据包不能传递到目标，**tracert** 命令将显示成功转发数据包的最后一个路由器。当数据报从我们的计算机经过多个网关传送到目的地时，**Tracert** 命令可以用来跟踪数据报使用的路由（路径）。该实用程序跟踪的路径是源计算机到目的地的一条路径，不能保证或认为数据报总遵循这个路径。如果我们的配置使用 **DNS**，那么我们常常会从所产生的应答中得到城市、地址和常见通信公司的名字。**Tracert** 是一个运行得比较慢的命令（如果我们指定的目标地址比较远），每个路由器我们大约需要给它 **15** 秒钟。

**Tracert** 的使用很简单，只需要在 **tracert** 后面跟一个 **IP** 地址或 **URL**，**Tracert** 会进行相应的域名转换的。

**tracert** 最常见的用法：

**tracert IP address [-d]** 该命令返回到达 **IP** 地址所经过的路由器列表。通过使用 **-d** 选项，将更快地显示路由器路径，因为 **tracert** 不会尝试解析路径中路由器的名称。

**Tracert** 一般用来检测故障的位置，我们可以用 **tracert IP** 在哪个环节上出了问题，虽然还是没有确定是什么问题，但它已经告诉了我们问题所在的地方，我们也就可以很有把握的告诉别人----某某地方出了问题。

**Tracert** 命令详解

该诊断实用程序将包含不同生存时间 (**TTL**) 值的 **Internet** 控制消息协议 (**ICMP**) 回显数据包发送到目标，以决定到达目标采用的路由。要在转发数据包上的 **TTL** 之前至少递减 **1**，必需路径上的每个路由器，所以 **TTL** 是有效的跃点计数。数据包上的 **TTL** 到达 **0** 时，路由器应该将“**ICMP** 已超时”的消息发送回源系统。**Tracert** 先发送 **TTL** 为 **1** 的回显数据包，并在随后的每次发送过程将 **TTL** 递增 **1**，直到目标响应或 **TTL** 达到最大值，从而确定路由。路由通过检查中级路由器发送回的“**ICMP** 已超时”的消息来确定路由。不过，有些路由器悄悄地下传包含过期 **TTL** 值的数据包，而 **tracert** 看不到。

**tracert [-d] [-h maximum\_hops] [-j computer-list] [-w timeout] target\_name**

使用 **tracert** 跟踪网络连接

**Tracert**（跟踪路由）是路由跟踪实用程序，用于确定 **IP** 数据报访问目标所采取的路径。**Tracert** 命令用 **IP** 生存时间 (**TTL**) 字段和 **ICMP** 错误消息来确定从一个主机到网络上其他主机的路由。

**Tracert** 工作原理

通过向目标发送不同 **IP** 生存时间 (**TTL**) 值的“**Internet** 控制消息协议 (**ICMP**)”回应数据包，**Tracert** 诊断程序确定到目标所采取的路由。要求路径上的每个路由器在转发数据包之前至少将数据包上的 **TTL** 递减 **1**。数据包上的 **TTL** 减为 **0** 时，路由器应该将“**ICMP** 已超时”的消息发回源系统。

**Tracert** 先发送 **TTL** 为 **1** 的回应数据包，并在随后的每次发送过程将 **TTL** 递增 **1**，直到目标响应或 **TTL** 达到最大值，从而确定路由。通过检查中间路由器发回的“**ICMP** 已超时”的消息确定路由。某些路由器不经询问直接丢弃 **TTL** 过期的数据包，这在 **Tracert** 实用程序中看不到。



Tracert 命令按顺序打印出返回“ICMP 已超时”消息的路径中的近端路由器接口列表。如果使用 -d 选项，则 Tracert 实用程序不在每个 IP 地址上查询 DNS。

在下例中，数据包必须通过两个路由器（10.0.0.1 和 192.168.0.1）才能到达主机 172.16.0.99。主机的默认网关是 10.0.0.1，192.168.0.0 网络上的路由器的 IP 地址是 192.168.0.1。

```
C:\>tracert 172.16.0.99 -d
```

```
Tracing route to 172.16.0.99 over a maximum of 30 hops
```

```
1 2s 3s 2s 10.0.0.1
```

```
2 75 ms 83 ms 88 ms 192.168.0.1
```

```
3 73 ms 79 ms 93 ms 172.16.0.99
```

```
Trace complete.
```

用 tracert 解决问题

可以使用 tracert 命令确定数据包在网络上的停止位置。下例中，默认网关确定 192.168.10.99 主机没有有效路径。这可能是路由器配置的问题，或者是 192.168.10.0 网络不存在（错误的 IP 地址）。

```
C:\>tracert 192.168.10.99
```

```
Tracing route to 192.168.10.99 over a maximum of 30 hops
```

```
1 10.0.0.1 reports:Destination net unreachable.
```

```
Trace complete.
```

Tracert 实用程序对于解决大网络问题非常有用，此时可以采取几条路径到达同一个点。

Tracert 命令行选项

Tracert 命令支持多种选项，如下表所示。

```
tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name
```

-d 指定不将 IP 地址解析到主机名称。

-h maximum\_hops 指定跃点数以跟踪到称为 target\_name 的主机的路由。

-j host-list 指定 Tracert 实用程序数据包所采用路径中的路由器接口列表。

-w timeout 等待 timeout 为每次回复所指定的毫秒数。

target\_name 目标主机的名称或 IP 地址。

使用 tracert 命令跟踪路径

打开 命令提示符，然后键入：

```
tracert host_name
```

```
或者键入 tracert ip_address
```

其中 host\_name 或 ip\_address 分别是远程计算机的主机名或 IP 地址。

例如，要跟踪从该计算机到 [url]www.microsoft.com[url] 的连接路由，请在命令提示符键入：

```
tracert [url]www.microsoft.com[url]
```

注意

要打开“命令提示符”，请单击“开始”，指向“程序”、“附件”，然后单击“命令提示符”。

tracert 命令跟踪 TCP/IP 数据包从该计算机到其他远程计算机所采用的路径。tracert 命令使用 ICMP 响应请求并答复消息（和 ping 命令类似），产生关于经过的每个路由器及每个跃点的往返时间 (RTT) 的命令行报告输出。

如果 tracert 失败，可以使用命令输出来帮助确定哪个中介路由器转发失败或耗时太多。

参数

/d

指定不将地址解析为计算机名。

-h maximum\_hops

指定搜索目标的最大跃点数。

`-j computer-list`

指定沿 `computer-list` 的稀疏源路由。

`-w timeout`

每次应答等待 `timeout` 指定的微秒数。

`target_name`

目标计算机的名称

## 十、Route

大多数主机一般都是驻留在只连接一台路由器的网段上。由于只有一台路由器，因此不存在使用哪一台路由器将数据报发表到远程计算机上去的问题，该路由器的 **IP** 地址可作为该网段上所有计算机的缺省网关来输入。

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\zykun>route /?

Manipulates network routing tables.

ROUTE [-f] [-p] [command [destination]
        [MASK netmask] [gateway] [METRIC metric] [IF interface]

-f          Clears the routing tables of all gateway entries.  If this is
            used in conjunction with one of the commands, the tables are
            cleared prior to running the command.
-p          When used with the ADD command, makes a route persistent across
            boots of the system. By default, routes are not preserved
            when the system is restarted. Ignored for all other commands,
            which always affect the appropriate persistent routes. This
            option is not supported in Windows 95.
command     One of these:
            PRINT      Prints a route
            ADD        Adds a route
            DELETE     Deletes a route
            CHANGE     Modifies an existing route
destination Specifies the host.
MASK        Specifies that the next parameter is the 'netmask' value.
netmask     Specifies a subnet mask value for this route entry.
            If not specified, it defaults to 255.255.255.255.
gateway     Specifies gateway.
interface   the interface number for the specified route.
METRIC      specifies the metric, ie. cost for the destination.

All symbolic names used for destination are looked up in the network database
file NETWORKS. The symbolic names for gateway are looked up in the host name
database file HOSTS.

If the command is PRINT or DELETE. Destination or gateway can be a wildcard,
(wildcard is specified as a star '*'), or the gateway argument may be omitted.

If Dest contains a * or ?, it is treated as a shell pattern, and only
matching destination routes are printed. The '*' matches any string,
and '?' matches any one char. Examples: 157.*.1, 157.*, 127.*, *224*.

Diagnostic Notes:
    Invalid MASK generates an error, that is when <DEST & MASK> != DEST.
    Example> route ADD 157.0.0.0 MASK 155.0.0.0 157.55.80.1 IF 1
            The route addition failed: The specified mask parameter is invalid
            <Destination & Mask> != Destination.

Examples:

> route PRINT
> route ADD 157.0.0.0 MASK 255.0.0.0 157.55.80.1 METRIC 3 IF 2
            destination^      ^mask      ^gateway      metric^      ^
                                   Interface^

    If IF is not given, it tries to find the best interface for a given
    gateway.
> route PRINT
```

但是，当网络上拥有两个或多个路由器时，我们就不一定想只依赖缺省网关了。实际上我们可能想让我们的某些远程 IP 地址通过某个特定的路由器来传递，而其他的远程 IP 则通过另一个路由器来传递。

在这种情况下，我们需要相应的路由信息，这些信息储存在路由表中，每个主机和每个路由器都配有自己独一无二的路由表。大多数路由器使用专门的路由协议来交换和动态更新路由器之

间的路由表。但在有些情况下，必须人工将项目添加到路由器和主机上的路由表中。**Route** 就是用来显示、人工添加和修改路由表项目的。

一般使用选项：

·route print

本命令用于显示路由表中的当前项目，在单路由器网段上的输出；由于用 IP 地址配置了网卡，因此所有的这些项目都是自动添加的。

·route add

使用本命令，可以将信路由项目添加给路由表。例如，如果要设定一个到目的网络 209.98.32.33 的路由，其间要经过 5 个路由器网段，首先要经过本地网络上的一个路由器，器 IP 为 202.96.123.5，子网掩码为 255.255.255.224，那么我们应该输入以下命令：

```
route add 209.98.32.33 mask 255.255.255.224 202.96.123.5 metric 5
```

·route change

我们可以使用本命令来修改数据的传输路由，不过，我们不能使用本命令来改变数据的目的地。下面这个例子可以将数据的路由改到另一个路由器，它采用一条包含 3 个网段的更直的路径：

```
route add 209.98.32.33 mask 255.255.255.224 202.96.123.250 metric 3
```

·route delete

使用本命令可以从路由表中删除路由。例如：route delete 209.98.32.33

### **NBTStat**

使用 nbtstat 命令释放和刷新 NetBIOS 名称。NBTStat (TCP/IP 上的 NetBIOS 统计数据) 实用程序用于提供关于关于 NetBIOS 的统计数据。运用 NetBIOS，我们可以查看本地计算机或远程计算机上的 NetBIOS 名字表格。

常用选项：

·nbtstat -n

显示寄存在本地的名字和服务程序。

·nbtstat -c

本命令用于显示 NetBIOS 名字高速缓存的内容。NetBIOS 名字高速缓存用于存放与本计算机最近进行通信的其他计算机的 NetBIOS 名字和 IP 地址对。

·nbtstat -r

本命令用于清除和重新加载 NetBIOS 名字高速缓存。

·nbtstat -a IP

通过 IP 显示另一台计算机的物理地址和名字列表，我们所显示的内容就像对方计算机自己运行 nbtstat -n 一样。

·nbtstat -s IP

显示实用其 IP 地址的另一台计算机的 NetBIOS 连接表。

例如我们在命令提示符下，键入：nbtstat -RR 释放和刷新过程的进度以命令行输出的形式显示。该信息表明当前注册在该计算机的 WINS 中的所有本地 NetBIOS 名称是否已经使用 WINS 服务器释放和续订了注册。

## 十一、NSLOOKUP

Nslookup 是一个监测网络中 DNS 服务器是否能正确实现域名解析的命令行工具。它在 Windows NT/2000/XP 中均可使用，但在 Windows 98 中没有集成这一个工具。

Nslookup 必须要安装了 TCP/IP 协议的网络环境之后才能使用。

现在网络中已经架设好了一台 DNS 服务器，主机名称为 ns-px.online.sh.cn，它可以把域名 http://www.jsjzx.net 解析为 220.181.31.3 的 IP 地址，这是我们平时用得比较多的正向解析功能。

检测步骤如下：

在 Windows 2000 中单击“开始”→“程序”→“附件”→“命令提示符”，在 C:\> 的后面键入 Nslookup www.jsjzx.net，“回车”之后即可看到如下结果：

Server: ns-px.online.sh.cn

Address: 202.96.209.5

Name: www.jsjzx.net

Address: 220.181.31.3

以上结果显示，正在工作的 DNS 服务器的主机名为 ns-px.online.sh.cn ，它的 IP 地址是 202.96.209.5 ，而域名 [www.jsjzx.net](http://www.jsjzx.net) 所对应的 IP 地址为 220.181.31.3 。那么，在检测到 DNS 服务器 ns-px.online.sh.cn 已经能顺利实现正向解析的情况下，它的反向解析是否正常呢？也就是说，能否把 IP 地址 220.181.31.3 反向解析为域名 www.jsjzx.net？我们在命令提示符 C:\> 的后面键入 **Nslookup 220.181.31.3** ，得到结果如下：

Server: ns-px.online.sh.cn

Address: 202.96.209.5

Name: www.jsjzx.net

Address: 220.181.31.3

这说明， DNS 服务器的反向解析功能也正常。

然而，有的时候，我们键入 Nslookup www.jsjzx.net ， 却出现如下结果：

Server: ns-px.online.sh.cn

Address: 202.96.209.5

**\*\*\* ns-px.online.sh.cn can't find www.jsjzx.net: Non-existent domain**

这种情况说明网络中 DNS 服务器 ns-px.online.sh.cn 在工作，却不能实现域名 www.jsjzx.net 的正确解析。此时，要分析 DNS 服务器的配置情况，看是否 **www.jsjzx.net** 这一条域名对应的 IP 地址记录已经添加到了 DNS 的数据库中。

还有的时候，我们键入 Nslookup www.jsjzx.net ， 会出现如下结果

**\*\*\* Can't find server name for domain: No response from server**

**\*\*\* Can't repair pc.nease.net : Non-existent domain**

这时，说明测试主机在目前的网络中，根本没有找到可以使用的 DNS 服务器。此时，我们要对整个网络的连通性作全面的检测，并检查 DNS 服务器是否处于正常工作状态，采用逐步排错的方法，找出 DNS 服务不能启动的根源。

## nslookup 命令用法

### 1.

```
*** Can't find server name for address 192.168.2.1: Non-existent domain
*** Default servers are not available
Server: UnKnown
Address: 192.168.2.1
```

```
Non-authoritative answer:
Name: www.cdnunion.com
Addresses: 61.129.102.61, 202.101.42.101
```

61.129.102.61, 202.101.42.101 是 WWW 对应的 IP 地址.

### 2.查询 MX 记录

```
C:\>nslookup -type=mx cdnunion.com
*** Can't find server name for address 192.168.2.1: Non-existent domain
*** Default servers are not available
Server: UnKnown
Address: 192.168.2.1
```

```
Non-authoritative answer:
cdnunion.com MX preference = 8, mail exchanger = mail.cdnunion.com
```

```
cdnunion.com nameserver = ns2.cdnunion.com
mail.cdnunion.com internet address = 61.129.102.61
```

mail.cdnunion.com 是 cdnunion.com 对应的 MX 记录.

### 3.查 CNAME 记录

```
C:\>nslookup -type=cname www.kukudm.com
*** Can't find server name for address 192.168.2.1: Non-existent domain
```

\*\*\* Default servers are not available

Server: UnKnown

Address: 192.168.2.1

Non-authoritative answer:

www.kukudm.com canonical name = www.kukudm.cdnunion.com

www.kukudm.cdnunion.com 是 www.kukudm.com 对应的 CNAME 记录.

#### 4.查询域名服务器

**C:\>nslookup -type=ns cdnunion.com**

\*\*\* Can't find server name for address 192.168.2.1: Non-existent domain

\*\*\* Default servers are not available

Server: UnKnown

Address: 192.168.2.1

Non-authoritative answer:

cdnunion.com nameserver = ns2.cdnunion.com

ns2.cdnunion.com internet address = 61.129.102.61

ns2.cdnunion.com 是 cdnunion.com 域名的 DNS 服务器.

#### 5.指定域名服务器查询结果.

**C:\>nslookup www.cdnunion.com 202.96.209.133**

Server: ns-pd.online.sh.cn

Address: 202.96.209.133

Non-authoritative answer:

Name: www.cdnunion.com

Address: 210.51.25.233

202.96.209.133 是上海 DNS 服务器 IP