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。作为一个生活在网络上的管理员或者黑客来说，ping命令是第一个必须掌握的DOS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。下面就来看看它的一些常用的操作。先看看帮助吧，在DOS窗口中键入：ping /? 回车，出现如图1。所示的帮助画面。在此，我们只掌握一些基本的很有用的参数就可以了（下同）。

-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，如图2。

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

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，只要你知道了远程主机的机器名称，就可以得到它的NETBIOS信息如图3（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

这是一个用来查看网络状态的命令，操作简便功能强大。

-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，可以知道机器所开的服务等信息，如图4。

这里可以看出本地机器开放有FTP服务、Telnet服务、邮件服务、WEB服务等。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。

四，tracert

跟踪路由信息，使用此命令可以查出数据从本地机器传输到目标主机所经过的所有途径，这对我们了解网络布局和结构很有帮助。如图5。

这里说明数据从本地机器传输到192.168.0.1的机器上，中间没有经过任何中转，说明这两台机器是在同一段局域网内。用法：tracert IP。

五，net

这个命令是网络命令中最重要的一个，必须透彻掌握它的每一个子命令的用法，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 /?回车如图6。

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。如图7。

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$连接（net use \IPIPC$ "password" /user:"name"），如图8。

建立了IPC$连接后，呵呵，就可以上传文件了：copy nc.exe \192.168.0.7admin$，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 servername，如图9，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，如图10。

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，如图11。

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，和图10进行比较就可以看出来。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，但我们还得知道。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。如图12。

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。如图13。

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），如图14。

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，如图15。

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，如图16。

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，就可以用它来干你想干的一切了。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，如图17。

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，如图18。

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，如图19。这里我使用的超级管理员权限登陆的。

DOS实际上是DiskOperationSystem（磁盘操作系统）的简称。顾名思义，这是一个基于磁盘管理的操作系统。与我们现在使用的操作系统最大的区别在于，它是命令行形式的，靠输入命令来进行人机对话，并通过命令的形式把指令传给计算机，让计算机实现操作的。所以操作方式也非常简单，只需输入命令，然后回车，系统就会执行命令。

 从实质上来说，包括windows95和win9x的系列版本，这些看起来完全图形化的操作系统也完全是建立在dos之上的。只是穿了一件衣服而已。

 另外一个方面，在widows的系列任意一个版本中，我们都可以找到dos的影子。在Win9x/Me的开始菜单中的运行程序中键入"command"命令，可进入命令行界面。在Win2000/NT的开始菜单中的运行程序中键入"cmd"命令，可进入命令行界面。而且使用windows 2000和xp都可以通过使用启动光盘来进入控制台。控制台也是命令行形式，里面的系统维护命令也是在很大程度上和DOS命令是一致的，如果会使用dos，基本上就会使用控制他。在很多情况下，使用图形界面不能妥善解决的问题，可以通过命令行来解决。

 需要强调的一点是命令行程序分为内部命令和外部命令，内部命令是随command.com装入内存的，而外部命令是一条一条单独的可执行文件。

 内部命令都集中在根目录下的command.com文件里，电脑每次启动时都会将这个文件读入内存，也就是说在电脑运行时，这些内部命令都驻留在内存中，用dir命令是看不到这些内部命令的。

外部命令都是以一个个独立的文件存放在磁盘上的，它们都是以com和exe为后缀的文件，它们并不常驻内存，只有在电脑需要时，才会被调入内存。

 一、目录操作命令：

 1.DIR

 DIR是英文单词directory(目录）的缩写，主要用来显示一个目录下的文件和子目录。

 [功能] 显示指定磁盘、目录中的文件和子目录信息，包括文件及子目录所在磁盘的卷标、文件与子目录的名称、每个文件的大小、文件及目录建立的日期时间，以及文件子目录的个数、所占用总字节数以及磁盘上的剩余总空间等信息。

 [格式] dir [C:][path][filename][.ext][/o][/s][/p][/w][/a]

 [说明] dir是DOS命令中最常用的一个。斜杠表示后面的内容是参数。

 参数意义

 /p 显示信息满一屏时，暂停显示，按任意键后显示下一屏

 /w 只显示文件名目录名，每行五个文件名。

 /s 将目录及子目录的全部目录文件都显示。如果是DIR 〔filename〕/s 作用是在当前栏目及下级各个子栏目中搜索符合条件的文件。

 [举例] 显示C:mybook目录里面的文件：DIR c:mybook\*.\*

 2. md

 md是英文make directory（创建目录）的缩写

 [功能] 创建一个子目录

 [格式] md [C:]path

 [举例] 用md 建立一个叫做mage的目录 md c:mage

3. cd

 cd是英文change directory(改变目录）的缩写

 [功能] 改变或显示当前目录

 [格式] cd [C:][path]

 [说明] 路径可以使用绝对路径和相对路径两种。如果只有cd而没有参数，则只显示当前路径。注意：子目录中一定有两个“特殊目录”，即“.”“..”，其中一点表示当前目录，两点表示上一层目录。从简单实用的角度来看，我们只要学会逐层进入（cd 下一层某目录名），和逐层退出（cd..）就可以解决所有问题。当然也可以用绝对路径的办法。

 [举例] 用cd转入刚才建立的mage目录 cd c:mage

 4. rd

 remove directory--删除目录

 [功能] 删除空子目录

 [格式] rd [d:]path

 [说明] rd是专门删除空子目录的命令。注意两条：一是不能删除非空目录；二是不能删除当前目录。

 [举例] 用rd删除mage这个目录。

 二、文件操作命令：

 5.copy 在英文中是复制的意思

 [功能] 复制一个或一组文件到指定的磁盘或目录中

 [格式] copy [C:][path][filename.ext] [C:][path]filename.ext

 [说明] 复制文件命令基本用法是：“复制源文件名目标文件名”。如果只写目标路径而不写目标文件名，表示同名复制；否则称为换名复制。注意：换名复制一般不要更改文件扩展名。

 [举例] 将C:mage目录的所有文件复制到软盘，可以打如下命令，请注意当前盘与当前路径不同：

 C:>copy c:mage\*.\* a:

 如果目标盘上已有同名文件，会出现如下提示，“Overwrite xxxx(Yes/No/All)”此时回答Y则覆盖当前文件，N则保留，A则覆盖此后的所有文件而不再提问。

 6. del

 del是英文delete（删除）的缩写

 [功能] 删除指定磁盘、目录中的一个或一组文件

 [格式] del [C:][path]filename.ext

 [说明] 这个命令应小心使用。一旦被删除，将不易恢复。同样可以采用通配符为删除一类文件。当利用\*.\*时，为了安全将给出警告，确定方进行删除工作。删除过程如没有信息提示，表示已正确删除。

 注意这个命令不能删除具有只读、隐含、系统属性的文件；如果指定文件不存在，则出现“File not found”的提示；DOS对误删除的文件可以用UNDELETE外部命令恢复；它只能删文件，不能删目录。

 7. ren

 ren是英文rename（重新命名）的简写

 [功能] 对指定磁盘、目录中的一个文件或一组文件更改名称

 [格式] ren [C:][path]filename1[.ext] filename2[.ext]

 [说明] 改名操作只限于某个文件某组文件的名称，它不会更改文件所在的目录。如果使用了通配符，则对一批文件进行更名。

8. type

 [功能] 在屏幕上显示文本文件内容命令

 [格式] type [C:][path]filename.ext

 [说明] type命令用来在屏幕上快速、简便地显示文本文件的内容，扩展名为TXT的文件是文本文件。如果用这个命令显示扩展名为EXE或COM等其它文件，输出的结果往往是一些乱七八糟的符号并伴有无规则的响铃声，有时甚至会出现死机现象。如果一屏显示不完的，可以使用在命令的尾部加上|more。

 三、磁盘操作命令

 9. format

 [功能] 磁盘格式化

 [格式] [C:][path]format drive:[/S]

 [说明] 厂家制造的各种磁盘可用来存储各种操作系统下的文件。不同操作系统的磁盘格式一般是不相同的，是不通用的。format命令就是使一个新的磁盘可以被DOS操作系统识别，即可存储DOS文件。

 这个命令对磁盘的格式化过程，实际上是用DOS规定的信息存储格式对磁盘进行规划的过程。格式化磁盘时，要清除磁盘上已经存在的所有数据，在磁盘上写上引导记录，划分出文件分配表和根目录，同时，它还要找出磁盘上的所有坏扇区并作上不可使用的标记。命令参数我们这里只列出了一个：/S。当使用了这个参数后，磁盘格式化并装入操作系统文件，使之变成引导盘。相当于format后再进行下一命令：SYS。

 10. discopy

 diskcopy，翻译成中文就是磁盘复制

 [功能] 复制出一个和原来磁盘内容一模一样的磁盘。

 [格式] diskcopy 源驱动器名目的驱动器名

 [说明] 特点在于是磁道对磁道的完全复制。它的主要用途就是用来备份。比如我们的电脑在刚买来时，会随机附带一些设备驱动程序磁盘，这些驱动程序在以后都有可能用到，为防止这些磁盘的损坏，一定要将它们都备份一套，这时，使用diskcopy命令是比较快捷和方便的。

 11. deltree

 [功能] 删除目录树

 [格式] [C:][path]DELTREE [C1:][path1] [[C2:][path2] […]]

 [说明] 这个命令将整个指定目录树全部消灭，而不管它是否是只读、隐藏与否。使用应特别小心。它是一个危险命令。

 12. chkdsk

 chkdsk是check disk的缩写。

 [功能] 用来检查你的磁盘的使用情况。

 [格式] chkdsk 磁盘名

 [说明] 例如要检查A盘使用情况，就输入chkdsk A: ，检查c盘使用情况，就输入chkdsk C: ，如果直接输入chkdsk，就检查当前磁盘的使用情况

 13. sys

 [功能] 传递系统文件命令。将DOS的两个隐含的系统IO.SYS和MSDOS.SYS传送到目标磁盘的特定位置上，并将COMMAND.COM文件复制过去。完成后，目标盘成为DOS的启动盘。

 [格式] [C:][path]SYS [C1:][path] d2:

 [说明] 由于这几个文件需要复制到特定位置上，所以用COPY命令完成的复制未必能够启动机器。能过SYS命令，DOS可以将目标盘已占据特定位置的文件移动，并将系统文件复制到相应位置上。参数C1:path用来指明系统文件所在目录。如不指明，则缺省为当前盘的当前目录。所以这个命令一般要在源盘的根目录进行。

本来，DOS讲完命令之后就应该结束了，但是考虑到现在上网的朋友，大都没有从基础上接触过DOS，也很少有在实际应用的环境下接触DOS的机会，所以特别讲一下DOS下的系统设备加载与系统环境设置，以便于大家真正的能使用DOS。

 首先要说的是，要进行DOS下的环境配置，基本上不可避免要使用到config.sys和AUTOEXEC.BAT这两个文件。Config.SYS文件是一个专业的系统启动配置文件，它主要用于加载内存管理程序、设置扩充内存及扩展内存、加载有关硬件驱动程序，设置有关环境变量等，为用户计算机的正常使用创造必要的用户环境(在DOS时代，精通Config.SYS文件往往是“专家”的标志)。（在Windows 95/98中，系统已经自带了内存管理、环境变量等设置功能，Config.sys文件的作用已经远远没有那么重要了，它仍在“服役”的原因主要是为了保持对老版本DOS应用程序的兼容）

 一些在config.sys中经常用到的配置项目如下：

 1、FILES＝数字

 表示可同时打开的文件数，一般可选择20到50，需要注意的是，如果把FILES的值设得过大会占用过多的基本内存。系统缺省为FILES=8。

 2、BUFFERS＝数字

 表示设置磁盘缓冲区的数目，通常设置为20-30左右。缺省值一般为15。磁盘缓冲区是一块内存区，用于存储从磁盘读入的数据或存储写到磁盘的数据。

 3、DEVICE和DEVICEHIGH

 用于加载一些内存驻留程序，用于管理设备。比如内存管理程序和光驱驱动程序等。如：

 DEVICE=C:＼DOS＼HIMEM.SYS

 DEVICE=C:＼DOS＼EMM386.EXE RAM

 DEVICEHIGH=C:＼CDROM＼CDROM.SYS

 DEVICEHIGH与DEVICE的不同是前者将程序加载入高端内存。

 4、HIMEM.SYS和EMM386.EXE

 DOS只能直接使用640KB的内存，即基本内存，必须依靠其他内存管理程序来使用更多的内存，这两条命令就是最常用的内存管理程序。

 其中640KB到1MB之间的内存被称为高端内存，是系统保留使用的。1MB以上的内存成为扩展内存，HIMEM.SYS就是负责管理扩展内存的。

 EMM386.EXE负责管理高端内存并在扩展内存中模拟扩充内存供某些软件使用。

 因此为了使用更多的内存，配置文件中应有以下指令。

 DEVICE=C:＼DOS＼HIMEM.SYS

 DEVICE=C:＼DOS＼EMM386.EXE RAM

 需要注意的是：EMM386.EXE必须要求先安装HIMEM.SYS，因而必须确保安装HIMEM.SYS的配置命令在EMM386.EXE之前。

 5、DOS＝HIGH，UMB

 一般情况下，需要CONFIG.SYS文件加入这条命令，这样会将DOS的系统文件移入高端内存，空出更多的基本内存给其他软件使用。需要注意的是，如果没有安装EMM386.EXE，UMB，那么这条指令将是无效的。

 下是一个典型的CONFIG.SYS文件内容：

 DEVICE=C:＼DOS＼HIMEM.SYS （加载himem，扩展内存管理器）

 DEVICE=C:＼DOS＼EMM386.EXE NOEMS （高端内存并入扩展内存的工具）

 BUFFERS=15,0          （缓冲区数目）

 FILES=50            （同时打开的文件数）

 DOS=UMB            （系统把DOS本身放在什么地方）

 LASTDRIVE=Z          （驱动器盘符最大可以用大哪个）

 DOS=HIGH

 DEVICEHIGH=C:＼DOS＼ATAPI\_CD.SYS /D:MSCD000 /I:0 （加载光驱驱动程序。）

 STACKS=9,256

 此外，在CONFIG中还可以配置菜单式多重任务选择的配置，用于不同任务的选择，比如玩游戏、设置虚拟磁盘等，不过在这些应用在目前已经不常用了，这里就不多做介绍了。

 有了config.sys以后，大部分的环境都能设置好，但是某些时候还是需要autoexec.bat来协作完成系统设备的加载，比如光驱。另外，有写设备直接使用命令来驱动的，就最好在autoexec.bat中执行来直接驱动，比如鼠标。

 下面是一个典型的autoexec.bat：

 关于AUTOEXEC.BAT

 电脑每次启动时都会自动寻找AUTOEXEC.BAT批处理文件，从而可执行一些每次开机都要执行的命令，比如设置路径PATH、加载鼠标驱动MOUSE、磁盘加速SMARTDRV等。

 下面给出一个比较典型的AUTOEXEC.BAT文件：

 @ECHO OFF '不显示命令行

 '设置提示符前有目录提示

 PROMPT &P& G

 PATH C:＼DOS;C:＼;C:＼WINDOWS; C:＼TOOLS '设置文件查找路径

 LH C:＼MOUSE＼MOUSE.COM

 '加载鼠标驱动程序

 LH C:＼DOS＼SMARTDRV.EXE

 '加载磁盘加速管理

 LH C:＼DOS＼MSCDEX /S /D:MSCD000/M:12 /V '加载CD-ROM驱动

 '设置临时目录

 SET TEMP=C:＼TEMP

 如果需要启动中文系统，也可以把中文系统的启动命令加入其中，自然启动以后就是中文的dos了。

 通过config.sys,autoexec.bat两个文件配合，完成绝大多数情况下DOS系统环境的配置。