必须掌握的八个DOS命令 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/136/2021_2022__E5_BF_85_E9_A1_BB_E6_8E_8C_E6_c98_136670.htm 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，。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。 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（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。 