黑客入门必须掌握 8 个 DOS 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。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。

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.

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: \\IP\sharename.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 $">\\192.168.0.7\admin$，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

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，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.

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.

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。

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。

。