




电脑软件 (/catalog.html)    单机游戏 (http://danji.cr173.com/)    安卓应用 (/android/)    安卓游戏 (http://azyx.cr173.com/)    苹果电脑 (/mac/)


苹果手机 (/list/r\_19\_1.html)

软件


搜索




石笼护坡



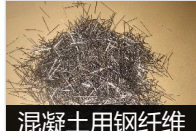
3d立体画




3dmax建模学习




水泥仿木栏杆




混凝土用钢纤维




树脂排水沟



广州艺考培训



发泡混凝土



软件工程师收广告

传播公益品牌，支持慈善事业  
为公益机构提供免费推广服务  
open.baidu.com

广告

首页 (/default\_cms.html) → 安全中心 (/artist/r\_5\_1.html) → 系统安全 (/artist/s\_29\_1.html) → 想成为电脑高手必须掌握的八个cmd 命令

## 想成为电脑高手必须掌握的八个cmd 命令


相关文章

发表评论

来源：宁宇 (http://blog.csdn.net/qjpspgf) 时间：2010/1/29 0:15:27 字体大小：A- A+ A+

作者：宁宇 点击：26869次 评论：10次 标签：

电脑 (/tags\_%B5%E7%C4%D4.html)



农场乐园探电脑版 (/game/203394.html) v1.1 安卓版

立即下载

(/game/203394.html)

类型：手游电脑版    大小：26.1M    语言：中文    评分：4.2

标签：

—, 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收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


### 推荐文章

没有数据

### 相关下载

	名称	大小	下载
1	农场乐园探电脑版	26.1M	<a href="#">下载</a>
2	10086视频直播电脑版	8.8M	<a href="#">下载</a>
3	100tv播放器电脑版	12.1M	<a href="#">下载</a>
4	100赚电脑版	12.7M	<a href="#">下载</a>
5	1010电脑版	21.3M	<a href="#">下载</a>
6	101教育PPT电脑版	195M	<a href="#">下载</a>
7	101随身学电脑版	4.2M	<a href="#">下载</a>
8	1024浏览器电脑版	42.0M	<a href="#">下载</a>
9	1031车主服务电脑版	12.7M	<a href="#">下载</a>
10	11个软件让你的电脑极速	325KB	<a href="#">下载</a>

### 最新文章



比SK PATCH/Loader激活  
windows7 更好更  
10-08-13  
 (/html/6024\_1.html)

正文内容

相关文章

发表评论

返回顶部

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 and 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。

正文内容  
相关文章  
发表评论  
返回顶部

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。

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。

最后，由衷的说一句，培养良好的安全意识才是最重要的。

=====

开始→运行→命令集锦

winver-----检查Windows版本

wmimgmt.msc----打开windows管理体系结构(WMI)

wupdmgr-----windows更新程序

wscript-----windows脚本宿主设置

write-----写字板

winmsd-----系统信息

wiaacmgr-----扫描仪和照相机向导

winchat-----XP自带局域网聊天

mem.exe-----显示内存使用情况

Msconfig.exe---系统配置实用程序

mplayer2-----简易widnows media player

mspaint-----画图板

mstsc-----远程桌面连接

mplayer2-----媒体播放机

magnify-----放大镜实用程序

mmc-----打开控制台

mobsync-----同步命令

dxdiag-----检查DirectX信息

drwtsn32----- 系统医生

devmgmt.msc--- 设备管理器

dfrg.msc-----磁盘碎片整理 (<http://www.cr173.com/k/cipansuipian/>)程序

diskmgmt.msc---磁盘管理实用程序

dcomcnfg-----打开系统组件服务

ddeshare-----打开DDE共享设置

dvdplay-----DVD播放器

net stop messenger-----停止信使服务

net start messenger----开始信使服务

notepad-----打开记事本

nslookup-----网络管理的工具向导

ntbackup-----系统备份和还原

narrator-----屏幕"讲述人"

正文内容

相关文章

发表评论

返回顶部

ntmsmgr.msc---移动存储管理器  
ntmsoprq.msc---移动存储管理员操作请求  
netstat -an----(TC)命令检查接口

syncapp-----创建一个公文包  
sysedit-----系统配置编辑器  
sigverif-----文件签名验证程序  
sndrec32-----录音机  
shrpublish-----创建共享文件夹  
secpol.msc-----本地安全策略  
syskey-----系统加密，一旦加密就不能解开，保护windows xp系统的双重密码  
services.msc---本地服务设置  
Sndvol32-----音量控制程序  
sfc.exe-----系统文件检查器  
sfc /scannow---windows文件保护

tsshutdown-----60秒倒计时关机命令  
tourstart-----xp简介（安装完成后出现的漫游xp程序）  
taskmgr-----任务管理器

eventvwr-----事件查看器  
eudcedit-----造字程序  
explorer-----打开资源管理器 (<http://www.cr173.com/k/zyqlq/>)

packager-----对象包装程序  
perfmon.msc---计算机性能监测程序  
progman-----程序管理器

regedit.exe----注册表  
rsop.msc-----组策略结果集  
regedt32-----注册表编辑器  
rononce -p ----15秒关机  
regsvr32 /u \*.dll----停止dll文件 (<http://www.cr173.com/k/dll/>)运行  
regsvr32 /u zipfldr.dll-----取消ZIP支持

cmd.exe-----CMD命令提示符  
chkdsk.exe----Chkdsk磁盘检查  
certmgr.msc---证书管理实用程序  
calc-----启动计算器 (<http://www.cr173.com/k/jisuanqi/>)  
charmap-----启动字符映射表  
cliconfg-----SQL SERVER 客户端网络实用程序  
Clipbrd-----剪贴板查看器  
conf-----启动netmeeting  
compmgmt.msc---计算机管理  
cleanmgr-----垃圾整理  
ciadv.msc-----索引服务程序

osk-----打开屏幕键盘  
odbcad32-----ODBC数据源管理器  
oobe/msoobe /a----检查XP是否激活  
lusrmgr.msc----本机用户和组  
logoff-----注销命令

iexpress-----木马捆绑工具，系统自带

Nslookup-----IP地址侦测器  
  
fsmgmt.msc-----共享文件夹管理器  
  
utilman-----辅助工具管理器  
  
gpedit.msc-----组策略

相关文章

我叫MT开荒团怎么在电脑上玩 我叫MT开荒团电脑版下载	08-19	微微一笑很倾城手游怎么在电脑上玩 微微手游电脑版安装	08-19
手机乐记事内容怎么同步到电脑乐云记事 乐云记事同步数	08-19	王者荣耀电脑版键位怎么设置 王者荣耀电脑版键位设置技	08-18
青云志手游怎么在电脑上玩 青云志手游电脑版下载安装教	08-17	玩图电脑版怎么设置？玩图电脑版怎么做分割字	08-15
微博电脑端突然不能登陆怎么回事 刷新微博刷不出来信息	08-09	王与异界骑士怎么在电脑上玩 王与异界骑士电脑版下载安	08-09
QQ电脑端火炬手图标怎么点亮 QQPC端火炬手图标点亮方	08-05	幻城手游怎么在电脑上玩 电脑版幻城手游下载安装教程	08-03


正文内容  
相关文章  
发表评论  
返回顶部



相关评论


阅读本文后您有什么感想? 已有 5343 人给出评价!

1506




喜欢

1056




顶

162




难过

1572




囧

236



围观

811



无聊

1 发泡混凝土

2 web安全培训

3 程序员怎么样

4 自动贴标机

5 水泥仿木栏杆

6 电脑编程入门自

7 移动公厕

8 unity3d特效

9 实验室通风橱

10 3dmax建模学习

11 程序员培训

12 软件工程师培训

13 400号码选号

14 实验室设备

15 网站开发

16 拉绳位移传感器

17 游戏编程要学什

18 电缆沟盖板

19 雨水收集

20 实验室建设

21 移动破碎站

22 软件工程师收入

23 3dmax培训班

24 3d培训班

广告

热门评论

最新评论

第 2 楼 本机地址CZ88.NET 网友 客人

发表于: 2015/10/24 8:09:36

高手 点赞!!!

支持( 0 ) 盖楼(回复)

第 1 楼 河南郑州郑州职业技术学院 网友 客人

发表于: 2014/4/10 20:00:55











好学易懂👍👍

支持( 0 ) 盖楼(回复)

发表评论

查看所有评论(10) (http://www.cr173.com/comment\_3917\_1.html)

昵称:

表情:          

字数: 0/500

发表评论

(您的评论需要经过审核才能显示)