

DOS 命令大全

dos 命令不区分大小写, 比如 C 盘的 Program Files, 在 dos 命令中完全可以用 "program files" 代替, 加上英文引号是因为名称的中间有空格(即多于一个词), 这一点是初学者经常忽略的。

DOS 特殊命令应用技巧:

- 1、向上箭头"↑"和向下箭头"↓"和向右箭头 —— 回看上一次执行的命令
- 2、"Ctrl+C" 组合键或 "Break" 键 —— 中断操作
- 3、鼠标操作 "标记" —— 用来选中文本
- 4、鼠标操作 "粘贴" —— 用来把剪贴板内容粘贴到提示符下
- 5、"F7" 键 —— 查看及执行用过的命令
- 6、"/?" —— 指定命令帮助
- 7、">" 及 ">>" —— 文件重定向

参数: 命令+ > +写入路径\文件名

实例:

echo 百度欢迎你 >d:\1.txt ; 写入文本到指定文件 (如果文件存在则替换)
netstat -an >>d:\1.txt ; 追随尾端写入文本

直接进入某盘符

直接进入某盘符, 盘符:

如直接进入 D 盘, D:

目录操作类命令

(一) md——建立子目录

1. 功能: 创建新的子目录
2. 类型: 内部命令
3. 格式: md[盘符:][路径名] <子目录名>
4. 使用说明:

(1) “盘符”: 指定要建立子目录的磁盘驱动器字母, 若省略, 则为当前驱动器;

(2) “路径名”: 要建立的子目录的上级目录名, 若缺省则建在当前目录下。

例: (1) 在 c 盘的根目录下创建名为 fox 的子目录; (2) 在 fox 子目录下再创建 user 子目录。

c: \>md fox (在当前驱动器 c 盘下创建子目录 fox)

c: \>md fox \user (在 fox 子目录下再创建 user 子目录)

(二) cd——改变当前目录

1. 功能: 改变当前目录
2. 类型: 内部命令
3. 格式: cd[盘符:][路径名][子目录名]
4. 使用说明:

(1) 如果省略路径和子目录名则显示当前目录; ver

(2) 如采用 “cd\” 格式, 则退回到根目录;

(3) 如采用 “cd..” 格式则退回到上一级目录。

例：(1) 进入到 user 子目录；(2) 从 user 子目录退回到子目录；(3) 返回到根目录。

c:\>cd fox\user (进入 fox 子目录下的 user 子目录)

c:\fox\user>cd.. (退回上一级根目录, 注意 cd 后面跟着两个点"..")。

c:\fox>cd\ (返回到根目录)

c:\

(三) rd——删除子目录命令

1. 功能：从指定的磁盘删除了目录。

2. 类型：内部命令

3. 格式：rd[盘符:][路径名][子目录名]

4. 使用说明：

(1) 子目录在删除前必须是空的，也就是说需要先进入该子目录，使用 del (删除文件的命令) 将其子目录下的文件删空，然后再退回到上一级目录，用 rd 命令删除该子目录本身；

(2) 不能删除根目录和当前目录。

例：要求把 c 盘 fox 子目录下的 user 子目录删除，操作如下：

第一步：先将 user 子目录下的文件删空；

c:\>del c:\fox\user*. * 或 del c:\fox\user 或 del c:\fox\user*

(注：这样只能删除文件，仍然不能删除 user 目录下的文件夹)

第二步，删除 user 子目录。

c:\>rd c:\fox\user

(注：如果 fox\user 文件夹下仍有文件夹，这一步将不会奏效，怎样解决呢？其实不必劳烦两步，直接这样 c:\>rd c:\fox\user /s

加上了一个参数/s，如果不想让系统询问是否删除，可以再加一个参数/q)。

rd (RMDIR)：在 DOS 操作系统中用于删除一个目录

RMDIR [/S] [/Q] [drive:]path

RD [/S] [/Q] [drive:]path

注意：以下两个参数只能在 WINXP 上使用（在 vista 系统下其实也可以使用下述两个参数！）

/S 除目录本身外，还将删除指定目录下的所有子目录和文件。用于删除目录树。

/Q 安静模式，带 /S 删除目录树时不要求确认。

如：删除 D 盘上名为 myfile (此文件夹是空的) 的文件夹，可以输入 rd d:\myfile。

如果 myfile 非空，可输入 rd d:\myfile /S d:\myfile 删除 myfile 文件夹及其所有子文件夹及文件。

(四) dir——显示磁盘目录命令

1. 功能：显示磁盘目录的内容。

2. 类型：内部命令

3. 格式：dir [盘符][路径][p][w]

4. 使用说明：/p 的使用；当欲查看的目录太多，无法在一屏显示完屏幕会一直往上卷，不容易看清，加上/p 参数后，屏幕上会分面一次显示 23 行的文件信息，然后暂停，并提示：press any key to continue

/w 的使用：加上/w 只显示文件名，至于文件大小及建立的日期和时间则都省略。加上参数后，每行可以显示五个文件名。

(五) path——路径设置命令

1. 功能：设备可执行文件的搜索路径，只对文件有效。
2. 类型：内部命令
3. 格式：path[盘符 1]目录[路径名 1][[: 盘符 2:], <目录路径名 2> ...]
4. 使用说明：

(1) 当运行一个可执行文件时，dos 会先在当前目录中搜索该文件，若找到则运行之；若找不到该文件，则根据 path 命令所设置的路径，顺序逐条地到目录中搜索该文件；

(2) path 命令中的路径，若有两条以上，各路径之间以一个分号“;”隔开；

(3) path 命令有三种使用方法：

path[盘符 1:][路径 1][盘符 2:][路径 2]... (设定可执行文件的搜索路径)

path: (取消所有路径)

path: (显示目前所设的路径)

(六) tree——显示磁盘目录结构命令

1. 功能：显示指定驱动器上所有目录路径和这些目录下的所有文件名。
2. 类型：外部命令
3. 格式：tree[盘符:][/f][>prn]
4. 使用说明：

(1) 使用/f 参数时显示所有目录及目录下的所有文件，省略时，只显示目录，不显示目录下的文件；

(2) 选用>prn 参数时，则把所列目录及目录中的文件名打印输出。

(七) deltree——删除整个目录命令

1. 功能：将整个目录及其下属于目录和文件删除。
2. 类型：外部命令
3. 格式：deltree[盘符:]<路径名>
4. 使用说明：该命令可以一步就将目录及其下的所有文件、子目录、更下层的子目录一并删除，而且不管文件的属性为隐藏、系统或只读，只要该文件位于删除的目录之下，deltree 都一视同仁，照删不误。使用时务必小心!!!

(八) tasklist——显示进程

1. 功能：将整个计算机的进程显示出来，同任务管理器。
2. 类型：外部命令
3. 格式：tasklist
4. 使用说明：运行 cmd tasklist

磁盘操作类命令

(一) format——磁盘格式化命令

1. 功能：对磁盘进行格式化，划分磁道和扇区；同时检查出整个磁盘上有无带缺陷的磁道，对坏道加注标记；建立目录区和文件分配表，使磁盘作好接收 dos 的准备。

2. 类型：外部命令
3. 格式：format <盘符:> [/s] [/4] [/q]

4. 使用说明:

(1) 命令后的盘符不可缺省, 若对硬盘进行格式化, 则会如下列提示:
warning:all data on non
——removable disk
drive c:will be lost !
proceed with format (y/n)?
(警告: 所有数据在 c 盘上, 将会丢失, 确实要继续格式化吗?)
(2) 若是对软盘进行格式化, 则会如下提示: insert new diskette for drive
a;
and press enter when ready...

(在 a 驱中插入新盘, 准备好后按回车键)。

(3) 选用[/s]参数, 将把 dos 系统文件 io.sys、msdos.sys 及 command.com 复制到磁盘上, 使该磁盘可以做为 dos 启动盘。若不选用/s 参数, 则格式化后的磁盘只能读写信息, 而不能做为启动盘;

(4) 选用[/4]参数, 在 1.2mb 的高密度软驱中格式化 360kb 的低密度盘;

(5) 选用[/q]参数, 快速格式化, 这个参数并不会重新划分磁盘的磁道和扇区, 只能将磁盘根目录、文件分配表以及引导扇区清成空白, 因此, 格式化的速度较快。

(6) 选用[/u]参数, 表示无条件格式化, 即破坏原来磁盘上所有数据。不加/u, 则为安全格式化, 这时先建立一个镜像文件保存原来的 fat 表和根目录, 必要时可用 unformat 恢复原来的数据。

(二) unformat 恢复格式化命令

1. 功能: 对进行过格式化误操作丢失数据的磁盘进行恢复。

2. 类型: 外部命令

3. 格式: unformat <盘符> [/l]/[u]/[p]/[test]

4. 使用说明: 用于将被“非破坏性”格式化的磁盘恢复。根目录下被删除的文件或子目录及磁盘的系统扇区(包括 fat、根目录、boot 扇区及硬盘分区表)受损时, 也可以用 unformat 来抢救。

(1) 选用/l 参数列出找到的子目录名称、文件名称、大孝日期等信息, 但不会真的做 format 工作。

(2) 选用/p 参数将显示于屏幕的报告(包含/l 参数所产生的信息)同时也送到打印机。运行时屏幕会显示: “print out will
be sent to lpt1”

(3) 选用/test 参数只做模拟试验(test)不做真正的写入动作。使用此参数屏幕会显示: “simulation only”

(4) 选用/u 参数不使用 mirror 映像文件的数据, 直接根据磁盘现状进行 unformat。

(5) 选用/psrtn; 修复硬盘分区表。

若在盘符之后加上/p、/l、/test 之一, 都相当于使用了/u 参数, unformat 会“假设”此时磁盘没有 mirror 映像文件。

注意: unformat 对于刚 format 的磁盘, 可以完全恢复, 但 format 后若做了其它数据的写入, 则 unformat 就不能完整的救回数据了。unformat 并非是万能的, 由于使用 unformat 会重建 fat 与根目录, 所以它也具有较高的危险性, 操作不当可能会扩大损失, 如果仅误删了几个文件或子目录, 只需要利用

undelete 就够了。

三) chkdsk——检查磁盘当前状态命令

1. 功能：显示磁盘状态、内存状态和指定路径下指定文件的不连续数目。

2. 类型：外部命令

3. 格式：chkdsk [盘符:][路径][文件名][/f][/v]

4. 使用说明：

(1) 选用[文件名]参数，则显示该文件占用磁盘的情况；

(2) 选[/f]参数，纠正在指定磁盘上发现的逻辑错误；

(3) 选用[/v]参数，显示盘上的所有文件和路径。

(四) diskcopy——整盘复制命令

1. 功能：复制格式和内容完全相同的软盘。

2. 类型：外部命令

3. 格式：diskcopy[盘符 1:][盘符 2:]

4. 使用说明：

(1) 如果目标软盘没有格式化，则复制时系统自动选进行格式化。

(2) 如果目标软盘上原有文件，则复制后将全部丢失。

(3) 如果是单驱动器复制，系统会提示适时更换源盘和目标盘，请操作时注意分清源盘和目标盘。

(五) label——建立磁盘卷标命令

1. 功能：建立、更改、删除磁盘卷标。

2. 类型：外部命令

3. 格式：label[盘符:][卷标名]

4. 使用说明：

(1) 卷标名为要建立的卷标名，若缺省此参数，则系统提示键入卷标名或询问是否删除原有的卷标名；

(2) 卷标名由 1 至 11 个字符组成。

(六) vol——显示磁盘卷标命令

1. 功能：查看磁盘卷标号。

2. 类型：内部命令

3. 格式：vol[盘符:]

4. 使用说明：省略盘符，显示当前驱动器卷标。

(七) scandisk——检测、修复磁盘命令

1. 功能：检测磁盘的 fat 表、目录结构、文件系统等是否有问题，并可将检测出的问题加以修复。

2. 类型：外部命令

3. 格式：scandisk[盘符 1:][[盘符 2:]...] [/all]

4. 使用说明：

(1) ccandisk 适用于硬盘和软盘，可以一次指定多个磁盘或选用[/all]参数指定所有的磁盘；

(2) 可自动检测出磁盘中所发生的交叉连接、丢失簇和目录结构等逻辑上的错误，并加以修复。

(八) defrag——重整磁盘命令

1. 功能：整理磁盘，消除磁盘碎块。

2. 类型：外部命令

3. 格式: defrag[盘符:][/f]

4. 使用说明: 选用/f 参数, 将文件中存在盘上的碎片消除, 并调整磁盘文件的安排, 确保文件之间毫无空隙。从而加快读盘速度和节省磁盘空间。

(九) sys——系统复制命令

1. 功能: 将当前驱动器上的 dos 系统文件 io. sys, msdos. sys 和 command. com 传送到指定的驱动器上。

2. 类型: 外部命令

3. 格式: sys[盘符:]

*使用说明: 如果磁盘剩余空间不足以存放系统文件, 则提示: no room for on destination disk.

文件操作类命令

(一) copy 文件复制命令

1. 功能: 拷贝一个或多个文件到指定盘上。

2. 类型: 内部命令

3. 格式: copy [源盘][路径] <源文件名> [目标盘][路径][目标文件名]

4. 使用说明:

(1) copy 是文件对文件的方式复制数据, 复制前目标盘必须已经格式化;

(2) 复制过程中, 目标盘上相同文件名称的旧文件会被源文件取代;

(3) 复制文件时, 必须先确定目标盘有足够的空间, 否则会出现; insufficient 的错误信息, 提示磁盘空间不够;

(4) 文件名中允许使用通配符 “*” “?”, 可同时复制多个文件;

(5) copy 命令中源文件名必须指出, 不可以省略。

(6) 复制时, 目标文件名可以与源文件名相同, 称作“同名拷贝”此时目标文件名可以省略;

(7) 复制时, 目标文件名也可以与源文件名不相同, 称作“异名拷贝”, 此时, 目标文件名不能省略;

(8) 复制时, 还可以将几个文件合并为一个文件, 称为“合并拷贝”, 格式如下: copy; [源盘][路径] <源文件名 1> <源文件名 2> ... [目标盘][路径] <目标文件名>;

(9) 利用 copy 命令, 还可以从键盘上输入数据建立文件, 格式如下: copy con [盘符:][路径] <文件名>;

(10) 注意: copy 命令的使用格式, 源文件名与目标文件名之间必须有空格!

(二) xcopy——目录复制命令

1. 功能: 复制指定的目录和目录下的所有文件连同目录结构。

2. 类型: 外部命令

3. 格式: xcopy [源盘:] <源路径名> [目标盘符:][目标路径名] [/s] [/v] [/e]

4. 使用说明:

(1) xcopy 是 copy 的扩展, 可以把指定的目录连文件和目录结构一并拷贝, 但不能拷贝隐藏文件和系统文件;

(2) 使用时源盘符、源目标路径名、源文件名至少指定一个;

(3) 选用/s 时对源目录下及其子目录下的所有文件进行 copy。除非指定 /e 参数, 否则/s 不会拷贝空目录, 若不指定/s 参数, 则 xcopy 只拷贝源目录本

身的文件，而不涉及其下的子目录；

(4) 选用/v 参数时，对拷贝的扇区都进行较验，但速度会降低。

(三) type——显示文件内容命令

1. 功能：显示 ascii 码文件的内容。

2. 类型：内部命令。

3. 格式：type[盘符:][路径]〈文件名〉

4. 使用说明：

(1) 显示由 ascii 码组成的文本文件，对.exe.com 等为扩展名的文件，其显示的内容是无法阅读的，没有实际意义；

(2) 该命令一次只可以显示一个文件的内容，不能使用通配符；

(3) 如果文件有扩展名，则必须将扩展名写上；

(4) 当文件较长，一屏显示不下时，可以按以下格式显示；type[盘符:][路径]〈文件名〉|more, more 为分屏显示命令，使用些参数后当满屏时会暂停，按任意键会继续显示。

(5) 若需将文件内容打印出来，可用如下格式：

type[盘符:][路径]〈文件名〉,>prn

此时，打印机应处于联机状态。

(四) ren——文件改名命令

1. 功能：更改文件名称

2. 类型：内部命令

3. 格式：ren[盘符:][路径]〈旧文件名〉〈新文件名〉

4. 使用说明：

(1) 新文件名前不可以加上盘符和路径，因为该命令只能对同一盘上的文件更换文件名；

(2) 允许使用通配符更改一组文件名或扩展名。

(五) fc——文件比较命令

1. 功能：比较文件的异同，并列出差异处。

2. 类型：外部命令

3. 格式：fc[盘符:][路径名]〈文件名〉[盘符:][路径名][文件名][a][c][n]

4. 使用说明：

(1) 选用/a 参数，为 ascii 码比较模式；

(2) 选用/b 参数，为二进制比较模式；

(3) 选用/c 参数，将大小写字符看成是相同的字符。

(4) 选用/n 参数，在 ascii 码比较方式下，显示相异处的行号。

(六) attrib——修改文件属性命令

1. 功能：修改指定文件的属性。(文件属性参见 2.5.4 (二) 文件属性一节)

2. 类型：外部命令。

3. 格式：attrib[文件名][r][—r][a][—a][h][—h][—s]

4. 使用说明：

(1) 选用 r 参数，将指定文件设为只读属性，使得该文件只能读取，无法写入数据或删除；选用—r 参数，去除只读属性；

(2) 选用 a 参数，将文件设置为档案属性；选用—a 参数，去除档案属性；

(3) 选用 h 参数，将文件调协为隐含属性；选用—h 参数，去隐含属性；

- (4) 选用 `s` 参数, 将文件设置为系统属性; 选用 `-s` 参数, 去除系统属性;
- (5) 选用 `/s` 参数, 对当前目录下的所有子目录及作设置。

七) `del`——删除文件命令

- 1. 功能: 删除指定的文件。
- 2. 类型: 内部命令
- 3. 格式: `del[盘符:][路径] <文件名> [/p]`
- 4. 使用说明:

(1) 不选用 `/p` 参数, 系统在删除前询问是否真要删除该文件, 若使用这个参数, 则自动删除;

(2) 该命令不能删除属性为隐含或只读的文件;

(3) 在文件名称中可以使用通配符;

(4) 若要删除磁盘上的所有文件 (`del *.*` 或 `del *`), 则会提示: (are you sure?) (你确定吗?) 若回答 `y`, 则进行删除, 回答 `n`, 则取消此次删除作业。

(八) `undelete`——恢复删除命令

- 1. 功能: 恢复被误删除命令
- 2. 类型: 外部命令。
- 3. 格式: `undelete[盘符:][路径名] <文件名> [/dos] [/list] [/all]`
- 4. 使用说明: 使用 `undelete` 可以使用 “*” 和 “?” 通配符。

(1) 选用 `/dos` 参数根据目录里残留的记录来恢复文件。由于文件被删除时, 目录所记载的文件名第一个字符会被改为 `e5`, `dos` 即依据文件开头的 `e5` 和其后续的字符来找到欲恢复的文件, 所以, `undelete` 会要求用户输入一个字符, 以便将文件名字补齐。但此字符不必和原来的一样, 只需符合 `dos` 的文件名规则即可。

(2) 选用 `/list` 只“列出”符合指定条件的文件而不做恢复, 所以对磁盘内容完全不会有影响。

(3) 选用 `/all` 自动将可完全恢复的文件完全恢复, 而不一一地询问用户, 使用此参数时, 若 `undelete` 利用目录里残留的记录来将文件恢复, 则会自动选一个字符将文件名补齐, 并且使其不与现存文件名相同, 选用字符的优选顺序为: `#%——0000123456789a~z`。

`undelete` 还具有建立文件的防护措施的功能, 已超出本课程授课范围, 请读者在使用些功能时查阅有关 `dos` 手册。

其它命令

(一) `cls`——清屏幕命令

- 1 功能: 清除屏幕上的所有显示, 光标置于屏幕左上角。
- 2 类型: 内部命令
- 3 格式: `cls`

(二) `ver` 查看系统版本号命令

- 1 功能: 显示当前系统版本号
- 2 类型: 内部命令
- 3 格式: `ver`

(三) `date` 日期设置命令

- 1 功能: 设置或显示系统日期。
- 2 类型: 内部命令

3 格式: date[mm——dd——yy]

4 使用说明:

(1) 省略[mm——dd——yy]显示系统日期并提示输入新的日期, 不修改则可直接按回车键, [mm——dd——yy]为“月月——日日——年年”格式;

(2) 当机器开始启动时, 有自动处理文件(autoexec.bat)被执行, 则系统不提示输入系统日期。否则, 提示输入新日期和时间。

(四) time 系统时钟设置命令

1 功能: 设置或显示系统时期。

2 类型: 内部命令

3 格式: time[hh: mm: ss: xx]

4 使用说明:

(1) 省略[hh: mm: ss: xx], 显示系统时间并提示输入新的时间, 不修改则可直接按回车键, [hh: mm: ss: xx]为“小时: 分钟: 秒: 百分之几秒”格式;

(2) 当机器开始启动时, 有自动处理文件(autoexec.bat)被执行, 则系统不提示输入系统日期。否则, 提示输入新日期和时间。

(五) mem 查看当前内存状况命令

1 功能: 显示当前内存使用的情况

2 类型: 外部命令

3 格式: mem[/c] [/f] [/m] [/p]

4 使用说明:

(1) 选用/c 参数列出装入常规内存和 cmb 的各文件的长度, 同时也显示内存空间的使用状况和最大的可用空间;

(2) 选用/f 参数分别列出当前常规内存剩余的字节大小和 umb 可用的区域及大小;

(3) 选用/m 参数显示该模块使用内存地址、大小及模块性质;

(4) 选用/p 参数指定当输出超过一屏时, 暂停供用户查看。

(六) msd 显示系统信息命令

1 功能: 显示系统的硬件和操作系统的状况。

2 类型: 外部命令

3 格式: msd[/s]

4 使用说明:

(1) 选用/i 参数时, 不检测硬件;

(2) 选用/b 参数时, 以黑白方式启动 msd;

(3) 选用/s 参数时, 显示出简明的系统报告。

ping 命令详解

对于 windows 下 ping 命令相信大家已经再熟悉不过了, 但是能把 ping 的功能发挥到最大的人却并不是很多, 当然我也并不是说我可以让 ping 发挥最大的功能, 我也只不过经常用 ping 这个工具, 也总结了一些小经验, 现在和大家分享一下。

现在我就参照 ping 命令的帮助说明来给大家说说我使用 ping 时会用到的技巧, ping 只有在安装了 tcp/ip 协议以后才可以使用:

ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [[-j computer-list] | [-k computer-list]] [-wz timeout]

destination-list

options:

-t ping the specified host until stopped.to see statistics and continue - type control-break;to stop - type control-c.

不停的 ping 地方主机，直到你按下 control-c。

此功能没有什么特别的技巧，不过可以配合其他参数使用，将在下面提到。

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 ***istrators 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：***istrator 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 用户登陆后用将密码改为 12345net 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 -annetstat -n 查看端口的网络连接情况,常用

netstat -annetstat -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”用于设置超时时间。

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

shutdown 命令

命令如下:

shutdown.exe -a 取消关机

shutdown.exe -s 关机

shutdown.exe -f 强行关闭应用程序。

shutdown.exe -m \\计算机名 控制远程计算机。

shutdown.exe -i 显示图形用户界面,但必须是 Shutdown 的第一个参数。

shutdown.exe -l 注销当前用户。

shutdown.exe -r 关机并重启。

shutdown.exe -t 时间 设置关机倒计时。

shutdown.exe -c“消息内容” 输入关机对话框中的消息内容(不能超 127 个字符)。

比如你的电脑要在 24:00 关机,可以选择“开始→运行”,输入“at 24:00 Shutdown -s”,这样,到了 24 点,电脑就会出现“系统关机”对话框,默认有 30 秒钟的倒计时并提示你保存工作。如果你想以倒计时的方式关机,可以输入“Shutdown.exe -s -t 7200”,这里表示 120 分钟后自动关机,“7200”代表 120 分钟。

如果想取消的话,可以在运行中输入“shutdown -a”。另外输入“shutdown -i”,则可以打开设置自动关机对话框,对自动关机进行设置。

让 Windows 2000 也实现同样的效果,可以把 Shutdown.exe 复制到系统目录 System32 下

eg:shutdown.exe -s -m \\z20235

当然你还可以把 shutdown 与 at 命配合使用来定时关机,会更加的精确,格式:at 关机时间 shutdown 选项

实例：at 12:45 shutdown -s -t 20 就是让机子在 12:45 关机，并倒计时 20 秒。须要注意的是在使用它时须先打开 “Task Scheduler” 服务。

八个基本 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。

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

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個，必須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。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。

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

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)。

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。

DOS 命令中字符的应用

一、单符号

【~】

① 在 for 中表示使用增强的变量扩展。

② 在 %var:~n,m% 中表示使用扩展环境变量指定位置的字符串。

③ 在 set/a 中表示一元运算符,将操作数按位取反。

【!】

① 在 set /a 中一元运算符,表示逻辑非。比如 set /a a=!0,这时 a 就表

示逻辑 1。

【@】

- ① 隐藏命令行本身的回显，常用于批处理中。

【\$】

- ① 在 findstr 命令里面表示一行的结束。
- ② 在 prompt 命令里面，表示将其后的字符转义（符号化或者效果化）。

【%】

- ① 在 set /a 中的二元运算符，表示算术取余。
- ② 命令行环境下，在 for 命令 in 前，后面接一个字符（可以是字母、数字或者一些特定字符），表示指定一个循环或者遍历指标变量。
- ③ 批处理中，后接一个数字表示引用本批处理当前执行时的指定的参数。
- ④ 其它情况下，%将会被脱去（批处理）或保留（命令行）

【^】

- ① 取消特定字符的转义作用，比如 & | > < ! " 等，但不包括 %。比如要在屏幕显示一些特殊的字符，比如 > > | ^ & 等符号时，就可以在其前面加一个 ^ 符号来显示这个 ^ 后面的字符了，^^ 就是显示一个 ^，^| 就是显示一个 | 字符了；
- ② 在 set /a 中的二元运算符，表示按位异或。
- ③ 在 findstr /r 的 [] 中表示不匹配指定的字符集。

【&】

- ① 命令连接字符。比如我要在一行文本上同时执行两个命令，就可以用 & 命令连接这两个命令。
- ② 在 set /a 中是按位与。

【*】

- ① 代表任意个任意字符，就是我们通常所说的“通配符”；比如想在 c 盘的根目录查找 c 盘根目录里所有的文本文件(.txt)，那么就可以输入命令 "dir c:*.txt"。
- ② 在 set /a 中的二元运算符，表示算术乘法。
- ③ 在 findstr /r 中表示将前一个字符多次匹配。

【-】

- ① 范围表示符，比如日期的查找，for 命令里的 tokens 操作中就可以用到这个字符。
- ② 在 findstr /r 中连接两个字符表示匹配范围。
- ③ -跟在某些命令的/后表示取反向的开关。
- ④ 在 set /a 中：
 - 1. 表示一个负数。
 - 2. 表示算术减运算。

【+】

- ① 主要是在 copy 命令里面会用到它，表示将很多个文件合并为一个文件，就要用到这个 + 字符了。
- ② 在 set /a 中的二元运算符，表示算术加法。

【:】

- ① 标签定位符，表示其后的字符串为以标签，可以作为 goto 命令的作用对象。比如在批处理文件里面定义了一个 ":begin" 标签，用 "goto begin" 命令就可以转到 ":begin" 标签后面来执行批处理命令了。

② 在`%var:string1=string2%`中分隔变量名和被替换字符串关系。

【|】

① 管道符，就是将上一个命令的输出，作为下一个命令的输入。`"dir /a/b |more"`就可以逐屏的显示 `dir` 命令所输出的信息。

② 在 `set/a` 中的二元运算符，表示按位或。

③ 在帮助文档中表示其前后两个开关、选项或参数是二选一的。

【/】

① 表示其后的字符（串）是命令的功能开关（选项）。比如`"dir /s/b/a-d"`表示`"dir"`命令指定的不同的参数。

② 在 `set/a` 中表示除法。

【>】

① 命令重定向符，

参数：命令+ > +写入路径\文件名

实例：

`echo 唐山味儿不浓 欢迎你 >d:\1.txt`；写入文本到指定文件（如果文件存在则替换）

② 在 `findstr/r` 中表示匹配单词的右边界，需要配合转义字符\使用。

【<】

① 将其后面的文件的内容作为其前面命令的输入。

② 在 `findstr/r` 中表示匹配单词的左边界，需要配合转义字符\使用。

【=】

① 赋值符号，用于变量的赋值。比如`"set a=windows"`的意思意思是将`"windows"`这个字符串赋给变量`"a"`。

② 在 `set/a` 中表示算术运算，比如`"set /a x=5-6*5"`。

【\】

① 这个`"\"`符号在有的情况下，代表的是当前路径的根目录。比如当前目录在 `c:\windows\system32` 下，那么你`"dir \"`的话，就相当与`"dir c:\"`。

② 在 `findstr/r` 中表示正则转义字符。

【,】

① 在 `set /a` 中表示连续表达式的分割符。

② 在某些命令中分割元素。

【.】

① 在路径的\后紧跟或者单独出现时：

一个.表示当前目录。

两个.表示上一级目录。

② 在路径中的文件名中出现时：

最后的一个.表示主文件名与扩展文件名的分隔。

【?】

① 在 `findstr/r` 中表示在此位置匹配一个任意字符。

② 在路径中表示在此位置通配任意一个字符。

③ 紧跟在/后表示获取命令的帮助文档。

【&&】

- ① 连接两个命令，当&&前的命令成功时，才执行&&后的命令。

【||】

- ① 连接两个命令，当||前的命令失败时，才执行||后的命令。

【>&】

- ① 将一个句柄的输出写入到另一个句柄的输入中。

【<&】

- ① 从一个句柄读取输入并将其写入到另一个句柄输出中。

【%%】

- ① 两个连续的%表示在预处理中脱为一个%。

② 批处理中，在 for 语句的 in 子句之前，连续两个%紧跟一个字符（可以是字母、数字和一些特定字符），表示指定一个循环或者遍历指标变量。

③ 批处理中，在 for 语句中，使用与 in 之前指定的指标变量相同的串，表示引用这个指标变量。

【>>】

- ① 命令重定向符，将其前面的命令的输出结果追加到其后面。

参数：命令+ >> +写入路径\文件名

实例：

echo 唐山味儿不浓 欢迎你 >d:\1.txt ;写入文本到指定文件（如果文件存在则替换）

netstat -an >>d:\1.txt ;即追随‘1.txt’的尾端继续写入‘netstat -an’命令输出结果

- ② 在 set /a 中的二元运算符，表示逻辑右移。

【==】

- ① 在 if 命令中判断==两边的元素是否相同。

【<<】

- ① 在 set /a 中的二元运算符，表示逻辑左移。

【+=】

① 在 set /a 中的二元运算符。例如 set /a a+=b 表示将 a 加上 b 的结果赋值给 a。

【-=】

① 在 set /a 中的二元运算符。例如 set /a a-=b 表示将 a 减去 b 的结果赋值给 a。

【*=】

① 在 set /a 中的二元运算符。例如 set /a a*=b 表示将 a 乘以 b 的结果赋值给 a。

【/=】

① 在 set /a 中的二元运算符。例如 set /a a/=b 表示将 a 加上 b 的结果赋值给 a。

【%=】

① 在 set /a 中的二元运算符。例如 set /a a%=b 表示将 a 除以 b 的余数赋值给 a。

注：命令行可以直接用 set /a a%=b，在批处理里面可以用 set /a a%%=b。

【^=】

① 在 set /a 中的二元运算符。例如 set /a a"^="b 表示将 a 与 b 按位异的结果赋值给 a。

注：这里 "^=" 加引号是为了防止^被转义，下同。

【&=】

① 在 set /a 中的二元运算符。例如 set /a a"&="b 表示将 a 与 b 按位与的结果赋值给 a。

【|=】

① 在 set /a 中的二元运算符。例如 set /a a"|="b 表示将 a 与 b 按位或的结果赋值给 a。

【<<=】

① 在 set /a 中的二元运算符。例如 set /a a"<<="b 表示将 a 按位左移 b 位的结果赋值给 a。

【>>=】

① 在 set /a 中的二元运算符。例如 set /a a">>="b 表示将 a 按位右移 b 位的结果赋值给 a。

【\<】

① 在 findstr 的一般表达式中表示字的开始处。

【\>】

① 在 findstr 的一般表达式中表示字的结束处。

【!!】

① 当启用变量延迟时，使用!!将变量名扩起来表示对变量值的引用。

【' '】

① 在 for/f 中表示将它们包含的内容当作命令行执行并分析其输出。

② 在 for/f "usebackq"中表示将它们包含的字符串当作字符串分析。

【()】

① 命令包含或者是具有优先权的界定符，比如 for 命令要用到这个()，我们还可以在 if, echo 等命令中见到它的身影。

② 在 set /a 中表示表达式分组。

【" "】

① 界定符，在表示带有空格的路径时常要用"来将路径括起来，在一些命令里面也需要" "符号。

② 在 for/f 中将表示它们包含的内容当作字符串分析。

③ 在 for/f "usebackq"表示它们包含的内容当作文件路径并分析其文件的内容。

④ 在其它情况下表示其中的内容是一个完整的字符串，其中的>、>>、<、&、|、空格等不再转义。

【` `】

① 在 for/f 中表示它们所包含的内容当作命令行执行并分析它的输出。

【[]】

① 在帮助文档表示其中的开关、选项或参数是可选的。

② 在 findstr /r 中表示按其中指定的字符集匹配

按住 shift 可少量输入大写字母，? +? 键表示先按住前一个键，同时按第二个键。

`ctrl+sc` 或 `ctrl+num lock` 暂停以便观察屏幕显示，在按一次继续。
`ctrl+c` 或 `ctrl+break` 终止程序运行，返回操作系统。