

网络安全技术应用丛书

畅销书《杀破狼》作者团队最新力作!

较量

——黑客命令全方位解析

武新华 李秋菊 张克歌 等编著

- ◆ Windows系统命令行及其配置
- ◆ Windows网络命令行
- ◆ 基于Windows认证的入侵与防御
- ◆ 远程管理Windows系统
- ◆ 来自局域网的攻击与防御
- ◆ 批处理BAT文件编程
- ◆ 病毒木马的主动防御和清除



附赠超值多媒体语音光盘



机械工业出版社
CHINA MACHINE PRESS

网络安全技术应用丛书

较量——黑客命令全方位解析

武新华 李秋菊 张克歌 等编著



机械工业出版社

本书紧紧围绕黑客命令与实际应用展开,详细剖析了黑客入侵过程中的相关命令,使读者对网络入侵防御技术形成系统了解,能够更好地防范黑客的攻击。全书共分为 11 章,内容包括:Windows 系统中的命令行,Windows 网络命令行,Windows 系统的命令行配置,基于 Windows 认证的入侵与防御,远程管理 Windows 系统,来自局域网的攻击与防御,做好网络安全防御,DOS 命令的实际应用,制作多种 DOS 启动盘,批处理 BAT 文件编程,病毒木马主动防御和清除等。

本书内容丰富,讲解深入浅出,图文并茂,不仅适用于广大网络爱好者,而且适用于网络安全从业人员及网络管理员。

图书在版编目(CIP)数据

较量——黑客命令全方位解析 / 武新华等编著. —北京:
机械工业出版社, 2009.6
(网络安全技术应用丛书)
ISBN 978-7-111-26752-2

I. 较… II. 武… III. 计算机网络-安全技术 IV.
TP393.08

中国版本图书馆 CIP 数据核字(2009)第 048971 号

机械工业出版社(北京市百万庄大街 22 号 邮政编码 100037)

策划编辑:丁 诚 吴鸣飞

责任编辑:吴鸣飞

责任印制:洪汉军

三河市国英印务有限公司印刷

2009 年 6 月第 1 版·第 1 次印刷

184mm×260mm·19.75 印张·485 千字

0001—4000 册

标准书号:ISBN 978-7-111-26752-2

ISBN 978-7-89451-058-7(光盘)

定价:42.00 元(含 1CD)

凡购本书,如有缺页、倒页、脱页,由本社发行部调换

销售服务热线电话:(010) 68326294 68993821

购书热线电话:(010) 88379639 88379641 88379643

编辑热线电话:(010) 88379753 88379739

封面无防伪标均为盗版

前言

黑客使用得最多、最频繁的工具，不是那些 Windows 系统中的工具软件，而是那些被 Microsoft 刻意摒弃的 DOS 命令，或者更具体点说，就是那些需要手工在命令行状态下输入的网络命令。因此，就有人不断发出“DOS 不是万能，但没有 DOS 是万万不能”的感慨。

在计算机技术日新月异的今天，称霸天下的 Windows 系统仍有很多做不了和做不好的事，学习和掌握 DOS 命令行技术仍然是进阶计算机高手的必修课程。

本书涵盖了 DOS 和 Windows 9x/ME/NT/2000/XP/2003/Vista 下几乎所有的网络操作命令，详细地讲解了各种命令的功能和参数，并针对具体应用列举了大量经典实例，能使广大 Windows 用户知其然，更知其所以然，真正做到学以致用，技高一筹。

为了省下用户宝贵的时间，提高用户的使用水平，本书在创作过程中力求体现如下特色。

- 从零起步，步步深入，通俗易懂地讲解，使初学者和具有一定基础的用户都能逐步提高，快速掌握黑客防范技巧与工具的使用方法。
- 注重实用性，理论和实例相结合，并配以大量插图和配套光盘视频讲解，力图使读者能够融会贯通。
- 介绍大量小技巧和小窍门，提高读者的效率，节省读者宝贵的摸索时间。
- 重点突出，操作简练，内容丰富，同时附有大量的操作实例，读者可以一边学习，一边在电脑上操作，做到即学即用、即用即得，让读者快速学会这些操作。

本书内容全面，语言简练，深入浅出，通俗易懂，既可作为即查即用的工具手册，也可作为了解系统的参考书目。本书不论在体例结构上，还是在技术实现及创作思想上，都做了精心的安排，力求将最新的技术、最好的学习方法、最快的掌握速度奉献给读者。

本书采用最为通俗易懂的图文解说，即使是电脑新手也能通读全书；任务驱动式的黑客软件讲解，揭秘每一种黑客攻击的手法；最新的黑客技术盘点，让读者实现“先下手为强”；攻防互参的防御方法，全面确保读者的网络安全。

参与本书编写的人员有武新华、李秋菊、张克歌、王英英、刘岩、段玲华、杨平、李防、陈艳艳、冯世雄、张晓新等。

本书在编写过程中得到了许多热心网友的支持，参考了部分来自网络的资料，并对这些资料进行了再加工和深化处理。在此对这些资料的原作者表示衷心的感谢。因为没有大家的共同努力，本书几乎是不可能完成的。

我们虽满腔热情，但限于自己的水平，书中的疏漏之处在所难免，欢迎广大读者批评指正。

最后，需要提醒大家的是：

根据国家有关法律规定，任何利用黑客技术攻击他人的行为都属于违法行为，希望读者在阅读本书后不要使用本书中介绍的黑客技术对别人进行攻击，否则后果自负。

目 录

前言

第 1 章 Windows 系统命令行基础	1
1.1 Windows 系统中的命令行	2
1.1.1 Windows 系统中的命令行概述	2
1.1.2 Windows 系统中的命令行操作	6
1.1.3 启动 Windows 系统中的命令行	6
1.2 在 Windows 系统中执行 DOS 命令	7
1.2.1 用菜单的形式进入 DOS 窗口	7
1.2.2 通过 IE 浏览器访问 DOS 窗口	7
1.2.3 编辑命令行	8
1.2.4 设置窗口风格	9
1.2.5 Windows Vista 系统命令行	11
1.3 全面认识 DOS 系统	12
1.3.1 DOS 系统的功能	12
1.3.2 文件与目录	12
1.3.3 文件类型与属性	13
1.3.4 目录与磁盘	15
1.3.5 命令分类与命令格式	16
1.4 IP 地址和端口	17
1.4.1 IP 地址概述	18
1.4.2 IP 地址的划分	18
1.4.3 端口的分类与查看	19
1.4.4 关闭和开启端口	22
1.4.5 端口的限制	23
1.5 可能出现的问题与解决	25
1.6 总结与经验积累	25
第 2 章 Windows 网络命令行	27
2.1 必备的几个内部命令	28
2.1.1 命令行调用的 Command 命令	28
2.1.2 复制命令 Copy	29
2.1.3 更改文件扩展名关联的 Assoc 命令	31
2.1.4 打开/关闭请求回显功能的 Echo 命令	33
2.1.5 查看网络配置的 Ipconfig 命令	33
2.1.6 命令行任务管理器的 At 命令	36
2.1.7 查看系统进程信息的 TaskList 命令	38

2.2 常用 Windows 网络命令行	40
2.2.1 测试物理网络的 Ping 命令	40
2.2.2 查看网络连接的 Netstat	42
2.2.3 工作组和域的 Net 命令	45
2.2.4 23 端口登录的 Telnet 命令	50
2.2.5 传输协议 FTP/Tftp 命令	51
2.2.6 替换重要文件的 Replace 命令	53
2.2.7 远程修改注册表的 Reg 命令	54
2.2.8 关闭远程计算机的 Shutdown 命令	57
2.3 其他的几个网络命令	58
2.3.1 Tracert 命令	58
2.3.2 Route 命令	59
2.3.3 Netsh 命令	61
2.3.4 Arp 命令	63
2.4 可能出现的问题与解决	64
2.5 总结与经验积累	65
第 3 章 Windows 系统命令行配置	67
3.1 Config.sys 文件配置	68
3.1.1 Config.sys 文件中的命令	68
3.1.2 Config.sys 配置实例	69
3.1.3 Config.sys 文件中常用的配置项目	70
3.2 批处理与管道	71
3.2.1 批处理命令实例	72
3.2.2 批处理中常用的命令	73
3.2.3 常用的管道命令	76
3.2.4 批处理的应用实例	78
3.3 对硬盘进行分区	80
3.3.1 硬盘分区的相关知识	80
3.3.2 利用 Diskpart 进行分区	82
3.4 可能出现的问题与解决	88
3.5 总结与经验积累	89
第 4 章 基于 Windows 认证的入侵与防御	91
4.1 IPC\$的空连接漏洞曝光	92
4.1.1 IPC\$概述	92
4.1.2 IPC\$空连接漏洞	93
4.1.3 IPC\$的安全解决方案	94
4.2 Telnet 高级入侵曝光	96
4.2.1 突破 Telnet 中的 NTLM 权限认证	97
4.2.2 Telnet 典型入侵曝光	99

4.2.3 Telnet 杀手锏	102
4.2.4 Telnet 高级入侵常用的工具	104
4.3 实现通过注册表入侵曝光	104
4.3.1 注册表的相关知识	105
4.3.2 远程开启注册表服务功能	107
4.3.3 连接远程主机的“远程注册表服务”	108
4.3.4 编辑注册表文件	109
4.3.5 通过注册表开启终端服务	113
4.4 实现 MS SQL 入侵曝光	116
4.4.1 用 MS SQL 实现弱口令入侵曝光	116
4.4.2 入侵 MS SQL 数据库曝光	120
4.4.3 入侵 MS SQL 主机曝光	120
4.4.4 MS SQL 注入攻击与防护	123
4.4.5 用 NBSI 软件实现 MS SQL 注入攻击曝光	124
4.4.6 MS SQL 入侵安全解决方案	126
4.5 获取账号密码曝光	128
4.5.1 用 Sniffer 获取账号密码曝光	128
4.5.2 字典工具曝光	133
4.5.3 远程暴力破解曝光	138
4.6 可能出现的问题与解决	140
4.7 总结与经验积累	140
第 5 章 远程管理 Windows 系统	141
5.1 实现远程计算机管理	142
5.1.1 计算机管理概述	142
5.1.2 连接到远程计算机并开启服务	143
5.1.3 查看远程计算机信息	144
5.1.4 用远程控制软件实现远程管理	147
5.2 远程命令执行与进程查杀	148
5.2.1 远程执行命令	148
5.2.2 查杀系统进程	149
5.2.3 远程执行命令方法汇总	151
5.3 FTP 远程入侵与安全解决方法	152
5.3.1 FTP 相关内容	152
5.3.2 扫描 FTP 弱口令	155
5.3.3 设置 FTP 服务器	155
5.4 可能出现的问题与解决	157
5.5 总结与经验积累	158
第 6 章 来自局域网的攻击与防御	159
6.1 Arp 欺骗与防御	160

6.1.1	Arp 欺骗概述	160
6.1.2	用 WinArpAttacker 实现 Arp 欺骗	161
6.1.3	网络监听与 Arp 欺骗	164
6.1.4	金山 Arp 防火墙的使用	165
6.1.5	AntiArp-DNS 防火墙	167
6.2	MAC 地址的克隆与利用	168
6.2.1	MAC 地址利用	168
6.2.2	MAC 地址克隆	171
6.3	Arp 广播信息	172
6.3.1	Netsend 攻击与防御	173
6.3.2	局域网助手 (LanHelper) 攻击与防御	174
6.4	断网攻击防范	177
6.4.1	DNS 服务器介绍	177
6.4.2	用 OpenDNS 解决断网问题	178
6.4.3	用网络守护神反击攻击者	180
6.5	可能出现的问题与解决	183
6.6	总结与经验积累	183
第 7 章	做好网络安全防御	185
7.1	建立系统漏洞体系	186
7.1.1	检测系统是否存在漏洞	186
7.1.2	如何修复系统漏洞	186
7.1.3	监视系统的操作过程	189
7.2	轻松防御间谍软件	191
7.2.1	轻松实现拒绝潜藏的间谍	191
7.2.2	用 Spybot 找出隐藏的间谍	192
7.2.3	出色的反间谍工具	195
7.2.4	间谍广告杀手	197
7.3	拒绝网络广告干扰	199
7.3.1	过滤弹出式广告傲游 Maxthon	199
7.3.2	过滤网络广告的广告杀手 Ad Killer	200
7.3.3	广告智能拦截的利器: Zero Popup	202
7.3.4	使用 MSN 的 MSN Toolbar 阻止弹出广告	203
7.4	拒绝流氓软件侵袭	204
7.4.1	Wopti 流氓软件清除大师	205
7.4.2	恶意软件清理助手	206
7.5	可能出现的问题与解决	207
7.6	总结与经验积累	208
第 8 章	DOS 命令的实际应用	209
8.1	DOS 命令的基础应用	210



8.1.1 在 DOS 下正确显示中文信息	210
8.1.2 恢复误删除文件	211
8.1.3 让 DOS 窗口无处不在	212
8.1.4 DOS 系统的维护	214
8.2 DOS 中的环境变量	215
8.2.1 SET 命令的使用	215
8.2.2 使用 DEBUG 命令	216
8.2.3 认识不同的环境变量	218
8.2.4 环境变量和批处理	220
8.3 在 DOS 中操作文件	221
8.3.1 抓取 DOS 窗口中的文本	221
8.3.2 在 DOS 中使用注册表	221
8.3.3 在 DOS 中实现注册表编程	222
8.3.4 在 DOS 中使用注册表扫描程序	223
8.4 网络中的 DOS 命令运用	224
8.4.1 检测 DOS 程序执行的目录	224
8.4.2 内存虚拟盘软件 XMS-DSK 的使用	225
8.4.3 在 DOS 中恢复回收站中的文件	226
8.4.4 在 DOS 中删除不必要的文件	226
8.5 可能出现的问题与解决	227
8.6 总结与经验积累	227
第 9 章 制作多种 DOS 启动盘	229
9.1 多种 DOS 启动盘的制作	230
9.1.1 Windows 版本的 DOS 启动盘	230
9.1.2 光盘版的 DOS 启动盘	231
9.1.3 U 盘版的 DOS 启动盘	233
9.1.4 硬盘版的 DOS 启动盘	235
9.1.5 制作多功能 DOS 启动光盘	238
9.2 DIY 自己的 Windows 2000/XP	242
9.2.1 NTFSDOS Pro 简介	243
9.2.2 NTFSDOS Pro 创建启动盘	243
9.3 用启动盘备份和修复系统	245
9.3.1 Windows 系统崩溃常见的类型	245
9.3.2 Windows 2000 的备份和修复	245
9.3.3 Windows XP 下的备份	248
9.4 可能出现的问题与解决	250
9.5 总结与经验积累	251
第 10 章 批处理 BAT 文件编程	253
10.1 在 Windows 中编辑批处理文件	254

10.2 在批处理文件中使用参数与组合命令	255
10.2.1 在批处理文件中使用参数	255
10.2.2 组合命令的实际应用	256
10.3 配置文件中常用的命令	258
10.3.1 分配缓冲区数目的 Buffers 命令	258
10.3.2 加载程序的 Device 命令	258
10.3.3 扩展键检查的 Break 命令	259
10.3.4 程序加载的 Devicehigh 命令	260
10.3.5 设置可存取文件数 Files 命令	260
10.3.6 安装内存驻留程序的 Install 命令	261
10.3.7 中断处理的 Stacks 命令	261
10.3.8 扩充内存管理程序 Himem.sys	262
10.4 用 BAT 编程实现综合应用	263
10.4.1 系统加固	263
10.4.2 删除日志	264
10.4.3 删除系统中的垃圾文件	264
10.5 Windows XP 开/关机脚本及其应用示例	265
10.5.1 指派开/关机脚本	265
10.5.2 开/关机脚本高级设置	267
10.5.3 开/关机应用示例	269
10.6 可能出现的问题与解决	273
10.7 总结与经验积累	274
第 11 章 病毒木马的主动防御和清除	275
11.1 关闭危险端口	276
11.1.1 通过安全策略关闭危险端口	276
11.1.2 自动优化 IP 安全策略	278
11.1.3 系统安全设置	282
11.2 用防火墙隔离系统与病毒	284
11.2.1 Windows 系统自带的防火墙	284
11.2.2 用“天网”将攻击挡在系统之外	287
11.2.3 ZoneAlarm 个人网络防火墙	292
11.3 对未知病毒木马全面监控	294
11.3.1 监控注册表与文件	295
11.3.2 监控程序文件	296
11.3.3 未知病毒木马的防御	298
11.4 可能出现的问题与解决	302
11.5 总结与经验积累	303

第1章

Windows 系统命令行基础

本章精粹

本章在讲解 Windows 系统命令行概述、作用以及在 Windows 系统中执行 DOS 命令的基础上,还介绍了 DOS 系统的功能、文件与目录属性、IP 地址和端口等内容,有助于读者掌握如何运用 Windows 系统中的命令行操作技巧,来维护计算机的正常工作。

重点提示

- Windows 系统命令行概述
- 在 Windows 系统中执行 DOS 命令
- 全面认识 DOS 命令
- IP 地址和端口

对于系统和网络管理者,繁杂的服务器管理及网络管理是日常工作的主要内容。网络越大,其管理工作强度就越大,管理难度也随之变大。传统窗口化的操作方式虽然容易上手,但对于技术熟练的管理人员,这些便利已成为一种“隐性”工作负担。因此,降低工作强度和管理难度就成为系统管理人员的最大问题,而命令行正好可以很好地解决这些问题。

1.1 Windows 系统中的命令行

随着互联网的普及,网络用户的逐渐增多,由此带来的安全问题正威胁着计算机的安全,而 Windows 操作系统本身都自带一些病毒和受残损的文件,常常影响用户无法正常工作。熟练掌握命令行的使用方法,将会使用户在 Windows 中得心应手,从而提高工作效率。因此,要想保障系统的稳定安全,就需要先掌握 Windows 系统中命令行的相关知识。

1.1.1 Windows 系统中的命令行概述

Windows 操作系统主要是用图形化界面,但是并不抛弃命令行的界面,但这个命令行界面就完全不是 DOS 操作系统了。同时 Windows 应用程序也分图形界面(包括无界面,如服务程序)和命令行界面。

命令行就是在 Windows 操作系统中打开 DOS 窗口,以字符串形式执行 Windows 管理程序。现在大部分用户都使用 Windows 的可视化界面,如果能够熟练掌握 Windows 系统中的命令行界面,将会更加占有优势。

Windows 系统中的命令行不少命令在用法上与 Windows 9x 的 DOS 命令相似,但它们的参数、功能、运行环境等却有了很大不同,有些命令已经不再是 16 位程序,而且有些命令还与图形界面浑然一体,甚至有些命令还能直接访问注册表信息。因此,应将 Windows XP 以后版本的 Windows 操作系统命令行控制台看作是图形界面不可缺少的补充。命令行程序分为内部命令和外部命令,内部命令是随 `command.com` 装入内存的,而外部命令是一条一条单独的可执行文件。

- 内部命令都集中在根目录下的 `command.com` 文件中,电脑每次启动时都会将这个文件读入内存,也即在电脑运行时,这些内部命令都驻留在内存中,用 `dir` 命令是看不到这些内部命令的。
- 外部命令都是以一个个独立的文件存放在磁盘上的,它们都是以 `com` 和 `exe` 为后缀的文件,并不常驻内存,只有在电脑需要时才会被调入内存。

在 Windows XP 以后版本的 Windows 操作系统下的 DOS 命令和一些其他功能,已经有所改变或增强。虽然两种操作都是使用命令来进行的,但由于命令行和纯 DOS 系统不是使用同一个平台,因此也存在一些区别。

下面以 Windows XP 为例讲述命令行的一些特殊功能(在 Windows XP 以后版本中 Windows 系统中,都拥有 Windows XP 中的功能),具体的表现如下:

1. 位置及地位特殊

命令程序已经不是专门用 `COMMAND` 目录存放,而是放在 32 位系统文件(Windows XP)安装目录下的 `SYSTEM32` 子目录中。由此可知,Windows XP 中的命令行命令已得到非常高的特殊地位,而且通过查看 `SYSTEM32\DLLCACHE` 目录可知,Windows XP 还将其

列入了受保护的系统文件之列，倘若 SYSTEM32 目录中的命令行命令受损，就用该 DLLCACHE 目录中的备份即可恢复。当然，由于 Windows XP 是“脱胎”于 Windows NT 的，因此，命令行调用主程序已不是 Windows 9x 时代的 COMMAND.COM，而是类似于 Windows NT 系统下的 CAM.EXE。

2. 一些命令只能通过命令行直接执行

Windows 9x 中的系统文件扫描器 sfc.exe 是一个 Windows 风格的对话框，而在 Windows XP 系统中，这条命令却必须在命令行状态手工输入才能按要求运行，而运行时又是标准的图形界面，如图 1-1 所示。



图 1-1 CMD 应用程序窗口

3. 命令行窗口的使用与以前大不相同

在窗口状态下，已经不再像 Windows 9x 的 DOS 窗口那样有一条工具栏，因此，不少人发现无法在 Windows XP 命令行窗口中进行复制、粘贴等操作。其实 Windows XP 命令行窗口是支持窗口内容选定、复制、粘贴等操作的，只是有关命令被隐藏了起来。用鼠标对窗口内容的直接操作只能是选取，即按下鼠标左键拖动时，其内容会反白显示，如果按〈Ctrl+C〉组合键，则无法将选取内容复制到剪贴板，而必须在窗口的标题栏上右键单击之后，再选择【编辑】选项，就可以在弹出的快捷菜单中看到复制、粘贴等选项了。

在 Windows XP 中的记事本或 Word 中输入“新北京，新奥运”信息之后，复制输入的内容并右键单击命令行标题栏，在弹出的快捷菜单中选择【粘贴】选项，即可将其粘贴到命令行窗口中，如图 1-2 所示。



图 1-2 命令行窗口内容复制图

还可以前后浏览每一步操作屏幕所显示的内容：这在全屏幕状态下是不可行的。必须使用〈Alt+Enter〉组合键切换到窗口状态，这时窗口右侧会出现一个滚动条，拖动滚动条就可前后任意浏览了。但如果操作的显示结果太多，则超过内存缓冲的内容将会按照 FIFO（First In First Out，先进先出）的原则自动丢弃，使用 CLS 命令后可以同时清除屏幕及缓冲区的内容。

4. 添加大量快捷功能键和类 DOSKEY 功能

在 Windows XP 操作系统的命令行状态下，通过“mem/c”命令看不到内存中自动加载 DOSKEY.EXE 命令的迹象，如图 1-3 所示。

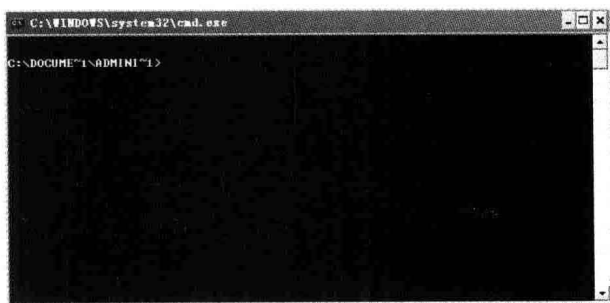


图 1-3 自动加载 DOSKEY 命令迹象图

具备类似传统的 DOSKEY 功能如下。

- PageUp、PageDown：重新调用最近的两条命令。
 - Insert：切换命令行编辑的插入与改写状态。
 - Home、End：快速移动光标到命令行的开头或结尾。
 - Delete：删除光标后面的字符。
 - Enter：复制窗口内选定的内容（用之取代〈Ctrl+C〉命令）。
 - F7：显示历史命令列表，可从列表中方便地选取曾经使用过的命令。
 - F9：输入命令号码功能，直接输入历史命令的编号即可使用该命令。
- 其他从〈F1〉～〈F9〉键都分别定义了不同的功能，具体操作时一试便知。

5. 对系统已挂接的码表输入法的直接支持

以前 Windows 9x 的 DOS 命令提示符下要显示和输入汉字，必须单独启动中文输入法，如 DOS 95 或 UC DOS 等其他汉字系统，在 Windows XP 的 CMD 命令行下已可以直接显示汉字，并按图形界面完全相同的热键，调用系统中已安装的各种码表输入法，如〈Ctrl+Shift〉组合键是切换输入法，〈Ctrl+Space〉组合键是切换输入法开关，〈Shift+Space〉组合键是切换全角与半角状态，〈Ctrl+.〉组合键是切换中英文标点等。不过，该命令行下的输入法只能在命令行中输入，比如打开了一个 Edit 编辑器，输入法就不起作用了。

6. CMD 的命令参数

CMD 的命令格式：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中断。
- /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。

- /q 关闭回应。
- /d 从注册表中停用执行 AUTORUN 命令。
- /t:fg 设置前景/背景颜色。
- /a 使向内部管道或文件命令的输出成为 ANSI。
- /e:on 启用命令扩展。
- /u 使向内部管道或文件命令的输出成为 Unicode。
- /e:off 停用命令扩展。
- /f:on 启用文件和目录名称完成字符。
- /f:off 停用文件和目录名称完成字符。
- /v:on 将 c 作为定界符启动延缓环境变量扩展。
- /v:off 停用延缓的环境扩展。

**【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。由于兼容原因，/x 与/e:on 相同，且/r 与/c 相同，忽略任何其他命令选项。

如果指定了/c 或/k 参数，命令选项后的命令行其他部分将作为命令行处理，在这种情况下，将使用下列逻辑处理引号字符（"）。

如果符合下列所有条件，则在命令行上的引号字符将被保留：

- 不带/s 命令选项。
- 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任意一个：<> () @ ^ |。
- 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。

否则，看第一个字符是否是一个引号字符，如果是，则舍去开头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 CAM 开始时，则会寻找 REG_SZ/REG_EXPAND_SZ 注册表变量。如果其中一个或两个都存在，则 HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\AutoRun 变量和 HKEY_CURRENT_USER\Software\Microsoft\Command Processor\EnableExtensions 变量将会先被执行到 0X1 或 0X0。用户特定设置有优先权，命令行命令选项比注册表设置有优先权。

7. 命令行扩展包括对命令的更改和添加

使用命令行扩展的命令主要有：DEL 或 ERASE、COLOR、CD 或 CHDIR、MD、MKDIR、PROMPT、PUSHD、POPD、SET SETLOCAL、ENDLOCAL、IF、FOR、CALL、SHIFT、GOTO、START、ASSOC、FTYPE 等。

延迟变量环境扩展不按默认值启用，可以用/v:on 或/v:off 参数，为某个启用或停用 CMD 调用的延迟环境变量扩充。也可在计算机上或用户登录会话上，启用或停用 CMD 所有调用的完成，这需要通过设置使用 Regedit32.exe 注册表中的一个或两个 REG_DWORD 值（HKEY_LOCAL_MACHINE\Software\Command processor\DelayedExpansion）和（HKEY_CURRENT_USER\Software\Microsoft\Command processor\DelayedExpansion）到 0X0 或 0X1 来实现。用户特定设置比计算机设置有优先权，命令行命令选项比注册表设置有优先权。

1.1.2 Windows 系统中的命令行操作

下面简单认识一下 Windows XP 操作系统中命令行的各种操作，例如复制、粘贴、设置属性等操作。当启动 Windows XP 中的命令行后，将会弹出【命令提示符】窗口。Windows 命令行跟 DOS 界面不一样，它会先显示当前操作系统的版本号，并把当前用户默认为当前提示符。而其下所使用的操作跟 DOS 命令中所作的操作一样，但在使用 Windows 命令时，可以自定义设置命令行的背景、显示的文字、窗口弹出的大小、窗口弹出的位置等。

右键单击命令行标题栏，将会弹出一个快捷菜单，在其中选择相应的菜单项，即可完成相应的操作，如图 1-4 所示。



图 1-4 命令行各种操作的快捷菜单

1.1.3 启动 Windows 系统中的命令行

不同的 Windows 操作系统版本，有不同的命令进入命令行界面，下面介绍两种不同启动 Windows 系统中命令行的方法：

- 在 Windows 2000/NT/XP/2003/Vista 操作系统的【运行】对话框中，在【打开】文本框中运行“cmd”命令，则可进入命令行窗口，如图 1-5 所示。



运行“cmd”后，将可以打开“命令提示符”窗口

图 1-5 命令提示符窗口

- 在 Windows 9x/Me 操作系统中的【运行】对话框中，在【打开】文本框中键入“command”命令，即可进入命令行窗口。

1.2 在 Windows 系统中执行 DOS 命令

由于 Windows 2000/XP/2003 彻底脱离了 DOS 操作系统，所以无法直接进入 DOS 环境，只能通过第三方软件来进行，如一键 GHOST 硬盘版等。但 Windows 2000/XP/2003 系统提供了一个“命令提示符”附件，可以提供基于字符的应用程序运行环境。通过使用类似 MS-DOS 命令解释程序中的各个字符和命令提示符来执行程序并在屏幕上显示输出。Windows 2000/XP/2003 命令提示符使用命令解释程序 cmd，将用户输入转化为操作系统可以理解的形式。

1.2.1 用菜单的形式进入 DOS 窗口

Windows 的图形化界面缩短了人与机器之间的距离，通过鼠标点击拖曳即可实现想要的功能。在 Windows 9x/Me 下，选择【开始】→【程序】→【附件】→【MS-DOS】菜单项，即可打开 DOS 窗口。

Windows XP 则是基于 OS/2、NT 构件的独立操作系统，除可以使用命令进入 DOS 环境外，还可以使用菜单方式打开【DOS 命令提示符】窗口。在 Windows XP 系统中选择【开始】→【程序】→【附件】→【命令提示符】菜单项，即可打开【命令提示符】窗口，如图 1-6 所示。



图 1-6 菜单进行 DOS 窗口

1.2.2 通过 IE 浏览器访问 DOS 窗口

用户可以直接在 IE 浏览器中调用可执行文件。对于不同阶段的操作系统，其通过 IE 浏览器访问 DOS 窗口的方法有所不同：

- 在 Windows 9x/Me 操作系统中访问 DOS 窗口，只需在 IE 浏览器地址栏中输入“c:\com mad.com”命令。
- 在 Windows 2000 操作系统中访问 DOS 窗口，只需在 IE 浏览器地址栏中输入