黑客技术典型应用系列

206分钟
DVD多媒体
讲解视频

黑客命令典型应用

武新华　孙世宁　等编著

- 揭秘网络安全攻防利器——黑客命令；知己知彼，全面保障网络安全。
- 通过典型实例全面解析黑客命令，应用环境、操作技巧和实战经验尽在其中。
- 网络安全高手点拨技术难点，精彩视频再现实战场景，全力弥补读者知识断层。

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

黑客技术典型应用系列

黑客命令与典型应用

武新华　孙世宁　等编著

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 简 介

本书紧紧围绕黑客命令的实际应用展开，剖析黑客攻防中迫切需要用到的命令，力求对其进行傻瓜式的讲解，使读者对网络入侵防御技术形成系统的了解，从而能够更好地防范黑客的攻击。全书共分为 11 章，包括：认识 Windows 系统中的命令行、常用 Windows 网络命令行、Windows 系统的命令行配置、实现基于 Windows 认证的入侵、远程管理 Windows 系统、系统进程与隐藏技术、留后门与清脚印技术、DOS 命令的实际应用、制作多种 DOS 启动盘、批处理 BAT 文件编程、木马病毒主动防御清除等内容。

本书内容丰富、图文并茂、深入浅出，适合网络管理员及网络安全从业人员阅读，也可作为广大网络安全爱好者的学习提升图书。

图书在版编目（CIP）数据

黑客命令与典型应用/武新华等编著. —北京：中国铁道出版社，2009.4
（黑客技术典型应用系列）
ISBN 978-7-113-09964-0

Ⅰ.黑… 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 062218 号

书　　名：黑客命令与典型应用
作　　者：武新华　孙世宁　等编著

策划编辑：严晓舟　荆　波
责任编辑：苏　茜　　**编辑部电话：**（010）63583215
编辑助理：惠　敏　　**封面制作：**白　雪
封面设计：付　巍
责任印制：李　佳

出版发行：中国铁道出版社（北京市宣武区右安门西街 8 号　　邮政编码：100054）
印　　刷：北京鑫正大印刷有限公司
版　　次：2009 年 6 月第 1 版　　2009 年 6 月第 1 次印刷
开　　本：787mm×1092mm　1/16　**印张：**20　**字数：**464 千
印　　数：4000 册
书　　号：ISBN 978-7-113-09964-0/TP・3248
定　　价：39.00 元（附赠光盘）

前 言

结束了白日喧嚣，繁华的都市像个玩累了的孩子慢慢安静下来，在静寂得令人窒息的黑夜里，都市的某个角落，微弱的光亮笼罩着一个不大的房间，黑暗中，显示屏不时地闪耀出深蓝色的光芒。一个人，一台笔记本，一杯热了又凉、凉了又热的咖啡，一根还没有抽完的烟，还有那台不知处于何处的服务器，依旧继续着……

长期以来，可能是受影视剧的影响，人们在潜意识中对“黑客”这个字眼十分敏感，认为黑客是不应该存在的，他们是网络的破坏者。一提起“黑客”，便会不由自主地浮现出上述联想。

其实，从客观存在的事实来看，黑客这类群体往往存在着一些共同点，如驱动他们成长的是对技术的无限渴望。一方面，黑客入侵可能造成网络的暂时瘫痪，另一方面，黑客也是整个网络安全完善的促进者，他们不知疲倦地寻找网络大厦的缺陷，使得网络大厦的根基更加稳固。

入侵者使用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，更具体地说，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 不是万能的，但没有 DOS 是万万不能的”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示例，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。

为了节省用户宝贵的时间，提高用户的使用水平，本书在创作过程中尽量达到以下特色：

- 从零起步，循序渐进由浅入深地讲解，使初学者和具有一定基础的用户都能逐步提高，快速掌握黑客命令的使用方法，达到防范黑客攻击的目的。
- 注重实用性，理论与实例相结合，并配以大量插图和配套光盘视频进行讲解，力图使读者能够将知识融会贯通。
- 介绍大量小技巧和小窍门，提高读者的学习效率，节省读者宝贵的时间。
- 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，让读者快速掌握所学知识。

本书内容全面、语言简练、深入浅出、通俗易懂，既适合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、最好的学习方法奉献给读者。

作者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，让用户实现“先下手为强”；攻防互参的防御方法，全面确保用户的网络安全。

本书由武新华、孙世宁等编著，其中武新华编写第 1 章，李伟编写第 2 章，曹燕华编写第 3 章，陈艳艳编写第 4 章，杨平编写第 5 章，段玲华编写第 6 章，张晓新编写第 7 章，刘岩编写第 8 章，王英英编写第 9 章，孙世宁编写第 10 章和第 11 章，最后由武新华统稿。本书在编

写过程中得到了许多热心网友的支持，参考了大量来自网络的资料，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！没有大家的共同努力，本书是不可能完成的。

我们虽满腔热情，但自己的水平有限，书中难免有疏漏之处，欢迎广大读者给予批评指正。

声明：

本书目的不是为那些怀有不良动机的人提供支持，也不承担因为技术被滥用所产生的连带责任。希望读者在阅读本书后，不要使用文中介绍的黑客技术对别人的主机进行攻击，否则后果自负。切记切记！

编　者

2009 年 4 月

目 录

第 1 章　认识 Windows 系统中的命令行

本章精粹

通过对本章的学习，读者可以掌握如何运用 Windows 系统中的命令行操作技巧来维护计算机的正常工作。为学习黑客防御措施奠定坚实的知识基础。

重点提示

- Windows 系统中的命令行。
- 在 Windows 系统中执行 DOS 命令。
- 全面认识 DOS 系统。
- IP 地址和端口。

黑客们使用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，更具体地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。

1.1　Windows 系统中的命令行

在计算机的具体应用过程中，使用 Windows 系统中的命令行操作可以方便、灵活、快速地查找并解决问题，实现某些正常的操作，从而保证用户能正常的工作。

Windows 操作系统主要应用图形化界面，但并不抛弃命令行界面。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。

1.1.1　Windows 命令行概述

命令行就是在 Windows 操作系统中打开 DOS 窗口，以字符串的形式执行 Windows 管理程序。尽管现在大多数用户都在使用 Windows 系统的可视化界面，但如果能够熟练掌握 Windows 系统中的命令行，将会更加占有优势。

虽然 Windows 2000 版本以后的 Windows 操作系统已断然抛弃了 DOS，但仍然提供对命令行控制台的支持，这可以从不同版本的操作系统进入命令行的操作中看出来。

命令行的不少命令在用法上与 Windows 9x 的 DOS 命令相似，但其参数、功能、运行环境等却有很大的不同。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，应当将 Windows XP 以后版本操作系统的命令行

控制台看做是图形界面不可缺少的补充。

在 Windows XP 以后版本操作系统下的 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 系统不使用同一个平台，因此也存在一些区别。

下面再来看看命令行的一些特殊功能（以 Windows XP 为例）。

1．位置及地位特殊

命令行程序已经不专门存放在 COMMAND 目录中了，而是存放在 32 位系统文件安装目录下的 SYSTEM32 子目录中。通过查看 SYSTEM32\DLLCACHE 目录可以知道，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，用该 DLLCACHE 目录中的备份可将其随即恢复。

当然，由于 Windows XP 脱胎于 Windows NT，所以命令行调用主程序已经不是 Windows 9X 时代的 COMMAND.COM，而是类似于 Windows NT 下的 CAM.EXE。

2．一些命令只能通过命令行直接执行

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

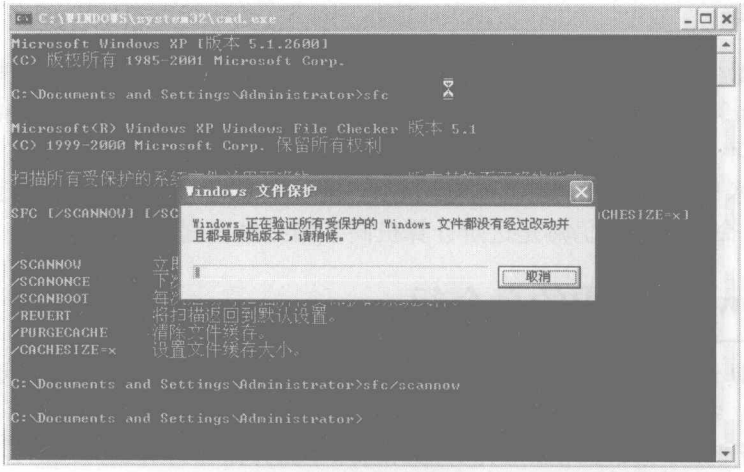

图 1-1　cmd 应用程序窗口

3．命令行窗口的使用与以前大不相同

Windows XP 命令行窗口已经不再像 Windows 9X 的 DOS 窗口那样有一条工具栏，因此无法在其中进行选定、复制、粘贴等操作。其实，Windows XP 的命令行窗口仍然支持窗口内容的选定、复制、粘贴等操作，只是有关命令被隐藏起来了。

用鼠标对窗口内容的直接操作只可是选取，即按下鼠标左键拖动时，其内容会反白显示，此时如果按【Ctrl+C】组合键，命令是无法将选取内容复制到剪贴板上的，而必须在窗口的标题栏上右击并选择“编辑”选项，才会看到有关复制、粘贴等操作命令的快捷菜单。

例如：要输入“2008 为北京奥运加油吧!!”信息，就可以在 Windows XP 中的记事本或 Word 文档中输入之后，再对其复制，然后在 Windows XP 中粘贴即可，如图 1-2 所示。

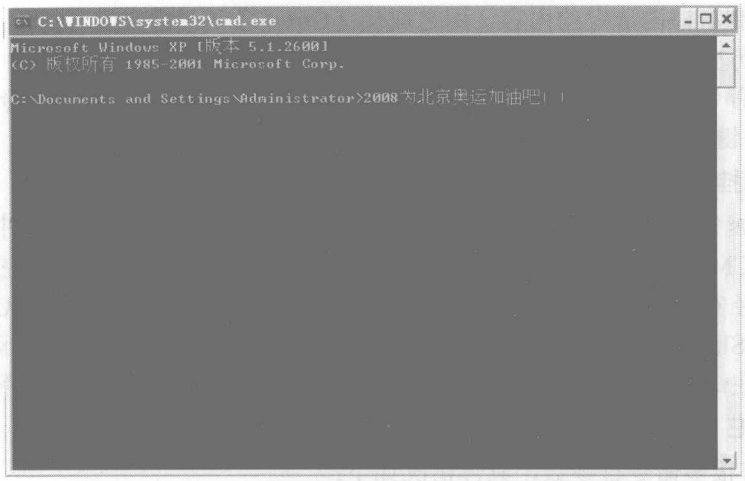

图 1-2　命令行窗口内容复制图

在全屏幕状态下浏览每一步操作屏幕上所显示的内容是不可行的。这必须使用【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，拖动滚动条即可前后任意浏览。但如果操作的显示结果太多，则超过内存缓冲的内容会按照 FIFO（First in First out，先进先出）的原则自动丢弃。使用 CLS 命令，可以同时清除屏幕及缓冲区的内容。

4．添加了大量快捷功能键和类 DOSKEY 功能

在 Windows XP 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。

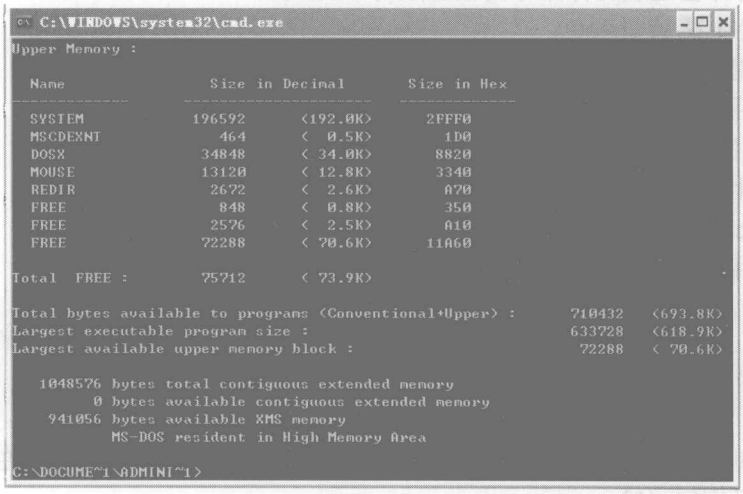

图 1-3　自动加载 DOSKEY 命令迹象图

但其的确具备极类似传统 DOSKEY 的功能，比如：

- PageUp、PageDown：重新调用最近的两条命令。
- Inter：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就可直接使用该命令。

其他 F1～F6 键及 F8 键都分别定义了不同的功能，具体操作试一试便知。

5．对系统已挂接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，而在 Windows XP 的 CMD.EXE 命令行下却可以直接显示汉字，并可按图形界面完全相同的热键直接调用系统中已经安装的各种码表输入法，如【Ctrl+Shift】键切换输入法，【Ctrl+Space】键切换输入法开关，【Shift+Space】键切换全角与半角状态，【Ctrl+.】切换中英文标点等。但命令行下的输入法只能在命令行进行输入，如果打开了一个 Edit 编辑器，输入法就不起作用了。

6．CMD.EXE 复杂、强大的命令参数

CMD.EXE 有很多命令行参数，具体情况如下：

```
CMD[a|u][/q][/d][/e:on|/e:off]][/t:fg][/f:on|/f:off][/v:on|/v:off][[/s][/c|/k]string]
```

参数说明：

- /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 ARTORUN 命令；
- /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；
- /e:on：启用命令扩展；
- /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。并由于兼容原因，/X 与/e:on 相同，/r 与/c 相同。

如果指定了/c 或/k，则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，会使用逻辑处理引号字符（"）。

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，其中特殊字符为下列中的任意一个：
  <> （） @^|
- 在两个引号字符之间至少有一个空白字符；

- 在两个引号字符之间至少有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，如果舍去开头的字符并删除命令行上最后一个引号字符，保留最后一个引号字符之后的文字。如果/d 在命令行上未被指定，则当 CAM.EXE 开始执行时，将会寻找以下 REG_SZ/REG_EXPAND_SZ 注册表变量。如果其中一个或两个都存在，则这两个变量将会先被执行。

HKEY_LOCAL_MACHINE\Software\Microsoft\Command Procssor\AutoRun 和 HKEY_CURRENT_USER\Software\Microsoft\Command Processor\EnableExtensions 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

命令行扩展包括对下列命令所做的更改和添加：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 命令选项为 CMD.EXE 的某个调用而启用或停用延迟环境变量扩充。

还可以在计算机上或用户登录会话上启用或停用 CMD.EXE 所有调用的事件，这要通过设置使用 Regedit32.exe 的注册表中的一个或两个 REG_DWORD 值来实现，如下所示。

HKEY_LOCAL_MACHINE\Software\Command processor\DelayedExpansion 和 HKEY_CURRENT_USER\Software\Microsoft\Command processor\DelayedExpansion 到 0X0 或 0X1。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　启动 Windows 命令行

不同版本的 Windows 操作系统，有不同的命令进入命令行界面。如 Windows 9X/Me 系统中，在“运行”对话框中输入 command 命令，即可进入命令行界面。而在 Windows 2000/NT/XP/2003/Vista 系统中，则须要在“运行”对话框中输入 cmd 命令，才可进入命令行界面，如图 1-4 所示。

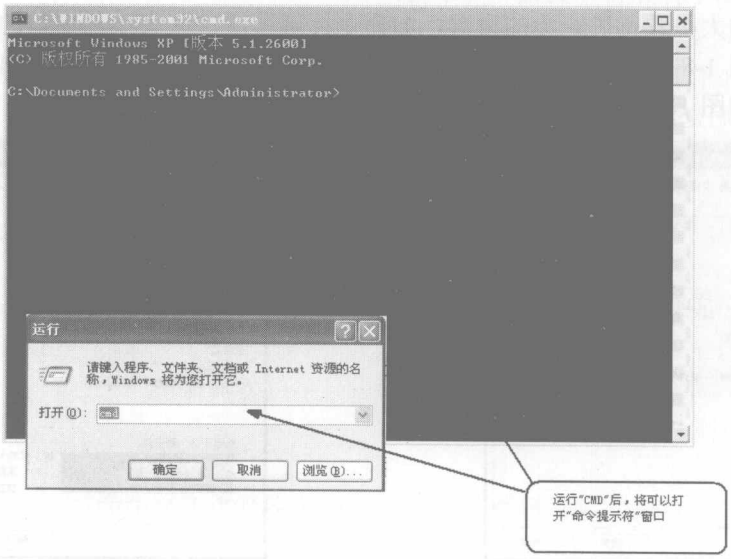

图 1-4　命令提示符窗口