本书采用最为通俗易懂的图文解说，即使您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，让您实现“先下手为强”
攻防互渗的防御方法，全面确保您的网络安全

矛与盾
黑客攻防命令大曝光

awk暗月　等编著

本书重点讲解

- Windows系统命令行基础
- Windows系统命令行配置
- 远程管理Windows系统
- DOS命令的实际应用
- 批处理BAT文件编程
- 常用Windows网络命令行
- 基于Windows认证的入侵
- 来自局域网的攻击与防御
- 制作启动盘
- 病毒木马的主动防御和清除

机械工业出版社
China Machine Press

矛与盾

黑客攻防命令大曝光

awk暗月　等编著

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

矛与盾：黑客攻防命令大曝光 / awk 暗月等编著. —北京：机械工业出版社，2013.7

ISBN 978-7-111-42929-6

Ⅰ. 矛… Ⅱ. a… 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（2013）第 131876 号

本书紧紧围绕黑客命令与实际应用展开，在剖析黑客入侵中用户迫切需要用到或迫切想要用到的命令时，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，能够更好地防范黑客的攻击。全书共分为 11 章，包括：Windows 系统命令行基础、常用 Windows 网络命令行、Windows 系统命令行配置、基于 Windows 认证的入侵、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 DOS 和 Windows PE 启动盘、批处理 BAT 文件编程，以及病毒木马的主动防御和清除等内容。

本书内容丰富、图文并茂、深入浅出，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。

机械工业出版社（北京市西城区百万庄大街 22 号 邮政编码 100037）

责任编辑：李 荣

三河市杨庄长鸣印刷装订厂印刷

2013 年 8 月第 1 版第 1 次印刷

186mm×240mm · 21.25 印张

标准书号：ISBN 978-7-111-42929-6

定 价：49.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

客服热线：（010）88378991 88361066 投稿热线：（010）88379604

购书热线：（010）68326294 88379649 68995259 读者信箱：hzjsj@hzbook.com

前　言

长期以来，人们在潜意识中已经对“黑客”这个字眼十分敏感，一提到“黑客”，人们便会不由自主地认为黑客是不应该存在的，他们是网络的破坏者。

其实，这是对“黑客”的一种极其片面的认识，因为从客观存在的事实来看，一方面，黑客入侵可能造成网络的暂时瘫痪，另一方面，黑客也是整个网络的建设者，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 命令行技术仍然是计算机高手进阶的必修课程。

本书涵盖 DOS 和 Windows 各版本操作系统下几乎所有的网络操作命令，详细地讲解各种命令的功能和参数，并针对具体应用列举大量经典示例，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。

为了给用户节省宝贵的时间，提高用户的使用水平，本书在创作过程中尽量满足以下几点要求：

- 从零起步、步步深入、通俗易懂、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，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，一边在计算机上操作，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、最好的学习方法奉献给读者。

作者采用最为通俗易懂的图文解说，即使是计算机新手也能读懂全书；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，攻防互渗的防御方法，全面确保网络安全。

本书由赵东升（awk 暗月）、陈艳艳和段玲华等编写，其中编写情况是：赵东升负责第 1 章，王英英负责第 2 章，冯世雄负责第 3 章，陈艳艳负责第 4 章，杨平负责第 5 章，段玲华负责第 6 章，张晓新负责第 7 章，李秋菊负责第 8 章，张克歌负责第 9 章，刘岩负责第 10 章，李防负责

第 11 章，最后由赵东升通审全稿。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。

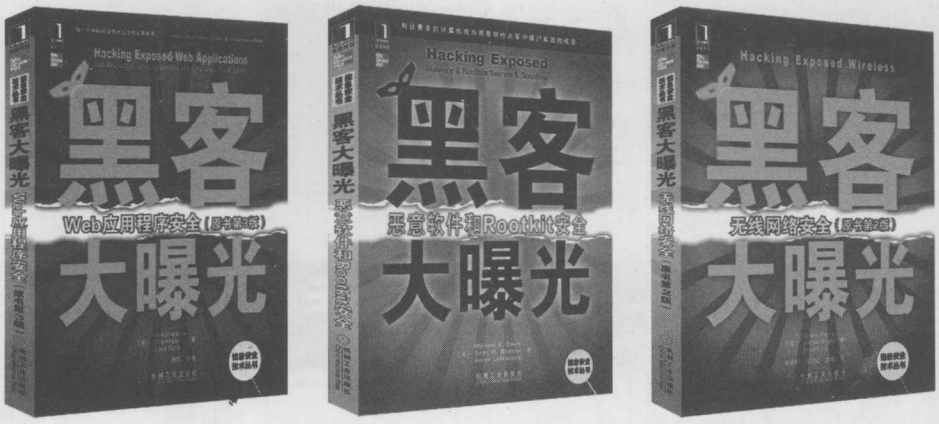
我们虽满腔热情，但限于自己的水平，书中的疏漏之处在所难免，欢迎广大读者批评指正。

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的系统进行攻击，否则后果自负，切记！

编　者

2013 年 6 月

推荐阅读



黑客大曝光：Web应用程序安全（原书第3版）

作者：（美）Joel Scambray 等 译者：姚军 等 ISBN：978-7-111-35662-2 定价：65.00元

黑客大曝光：恶意软件和Rootkit安全

作者：（美）Michael A. Davis 等 译者：姚军 等 ISBN：978-7-111-34034-8 定价：55.00元

黑客大曝光：无线网络安全（原书第2版）

作者：（美）Johnny Cache 等 译者：李瑞民 等 ISBN：978-7-111-37248-6 定价：69.00元

C++反汇编与逆向分析技术揭秘

作者：钱林松 等 ISBN：978-7-111-35633-2 定价：69.00元

网络扫描技术揭秘：原理、实践与扫描器的实现

作者：李瑞民 ISBN：978-7-111-36532-7 定价：79.00元

BackTrack 4：利用渗透测试保证系统安全

作者：Shakeel Ali 等 译者：陈雪斌 等 ISBN：978-7-111-36643-0 定价：59.00元

Windows PE权威指南

作者：戚利 ISBN：978-7-111-35418-5 定价：89.00元

内核漏洞的利用与防范

作者：Enrico Perla 等 译者：吴世忠 等 ISBN：978-7-111-37429-9 定价：79.00元

Java加密与解密的艺术

作者：梁栋 ISBN：978-7-111-29762-8 定价：69.00元

云计算安全与隐私

作者：Tim Mather 等 译者：刘戈舟 等 ISBN：978-7-111-34525-1 定价：65.00元

安全之美

作者：Andy Oram 等 译者：徐波 等 ISBN：978-7-111-33477-4 定价：65.00元

内容全面，详尽地剖析了Windows PE文件格式的原理及其编程技术

实践性强，以案例驱动的方式讲解了Windows PE文件格式在加密与解密、软件汉化、逆向工程、反病毒等安全领域的应用

Windows PE权威指南

作者：戚利 著　ISBN：978-7-111-35418-5　定价：89.00 元

本书内容针对性很强，学术研究和实践操作并重，不但适合计算机安全领域的初学者，对大专院校相关专业的学生也有很好的指导作用。本书表述方式生动准确，理论与实践并重，通过本书，读者既能很好地了解PE格式，又能在实际工作和研究过程中运用这些知识。因此，在本书付梓之际，感谢作者的辛勤付出，希望读者能够通过本书获得更多的收益！

——**段钢 看雪安全网站（www.pediy.com）创始人**

内容全面，全书围绕PE文件格式展开，不仅讲解了PE文件格式的原理和与之相关的编程技术和技巧，还以实例的方式讲解了PE文件格式在加密与解密、软件汉化、逆向工程、反病毒等安全领域的应用。注重实践，理论与案例相结合，不仅在各个知识点都辅有用以阐述理论的案例，而且还专门围绕PE的应用编写了多个具有商业价值的实用案例，这些案例相对完整且具有可扩展性和启发性。强烈推荐！

——**黑客反病毒组织（www.hackav.com）**

对于计算机领域的安全工作者而言，无论你是从事加密与解密、软件汉化相关的工作，还是从事逆向工程、反病毒相关的工作，都十分有必要系统而全面地掌握PE文件格式的原理和编程技术。本书内容全面，从原理到应用，涵盖了PE文件格式的方方面面；实战性强，不仅为每个知识点配备了便于读者理解的小案例，还提供了几个大型的商业案例；结构清晰，语言通俗易懂，可读性较强。十分难得！

——**51CTO（www.51cto.com）**

目 录

第 1 章　Windows 系统命令行基础

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

本章精粹

本章在讲述 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，以及 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。

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来说，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

随着因特网的普及，网络用户的逐渐增多，由此带来的安全问题也威胁着计算机安全，而 Windows 操作系统本身都自带一些病毒和受残损的文件，常常使用户无法正常工作。熟练掌握命令行的使用方法，将会使用户在 Windows 系统中的操作更加得心应手，从而提高工作效率。因此，要想保障系统的稳定安全，就需要首先掌握 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 操作系统主要用的是图形化界面，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。

命令行中的不少命令在用法上与 Windows 9X 的 DOS 命令相似，但它们的参数、功能和运行环境等却有很大不同，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做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，计算机每次启动时都会将这个文件读入内存，也即在计算机运行时，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 为扩展名的文件，并不常驻内存，只有在计算机需要时才会被调入内存。

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 以后版本的 Windows 系统中，都拥有 Windows XP 中的功能），具体表现如下。

1. 位置及地位特殊

命令行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，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，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。

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、复制和粘贴等操作的，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够是选取，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击，在弹出的快捷菜单中选择“编辑”命令，就可以在打开的子菜单中看到复制、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击命令行标题栏，在弹出的快捷菜单中选择“编辑”→“粘贴”命令，即可将其粘贴到命令行窗口中，如图 1-2 所示。

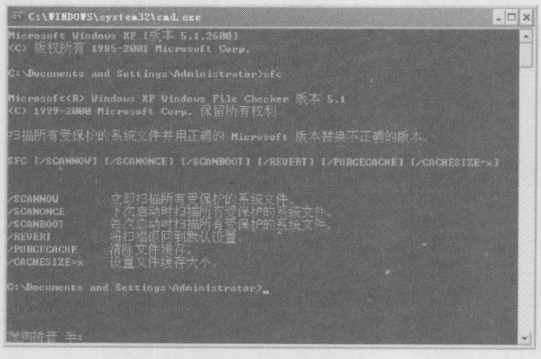


图 1-1　cmd 应用程序窗口

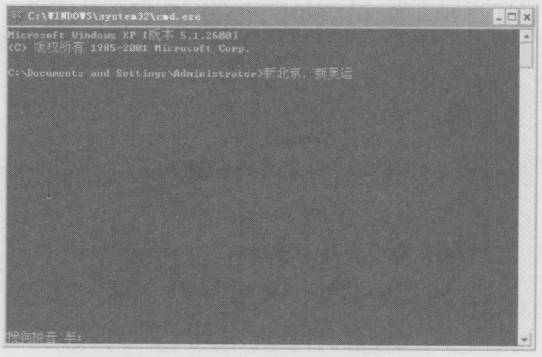


图 1-2　命令行窗口内容复制图

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，拖动滚动条就可以前后任意浏览了。但如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）的原则将自动丢弃，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。