Windows
网络安全技术专家
倾力巨献

赠 CD多媒体光盘

赠送作者编写的部分代码和工具

裴要强 孟 波 编著

Windows黑客技术揭秘与攻防 I

——C语言篇

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

裴要强　孟　波　编著

Windows 黑客技术揭秘与攻防 I

—C语言篇

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 简 介

本书对目前流行的 Windows 黑客编程技术逐一进行讲解，揭开黑客编程的神秘面纱。全书详细剖析了目前流行的各种黑客技术，包括文件操作技术、后门编程技术、扫描嗅探技术、木马下载者技术、U 盘小偷、密码盗窃、验证码的破解、进程控制技术、NTFS 数据流的检测与清除、系统监控技术、API Hook 与 SPI 等。另外，还讲解一些常见的安全防御编程。

本书集合了笔者的大量学习经验，并在写作时有所侧重，突出实用性，对引入的新知识都进行了详细的原理性介绍，使读者能够真正理解。

本书适合广大 Windows 编程爱好者、计算机安全从业人员、刚刚学会 C/C++语言并亲自编写过一些小型程序的读者。

图书在版编目（CIP）数据

Windows 黑客技术揭秘与攻防. 1，C 语言篇 / 裴要强，孟波编著. --北京：中国铁道出版社，2010.9

ISBN 978-7-113-11394-0

Ⅰ. ①W… Ⅱ. ①裴… ②孟… Ⅲ. ①计算机网络－安全技术②C 语言—程序设计 Ⅳ. ①TP393.08②TP312

中国版本图书馆 CIP 数据核字（2010）第 076186 号

书　　名：Windows 黑客技术揭秘与攻防Ⅰ——C 语言篇
作　　者：裴要强　孟　波　编著

策划编辑：苏　茜
责任编辑：韩中领　　**读者热线电话：400-668-0820**
特邀编辑：王　惠
封面设计：张　丽　　**封面制作：白　雪**
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：北京市兴顺印刷厂
版　　次：2010 年 9 月第 1 版　　2010 年 9 月第 1 次印刷
开　　本：787mm×1092mm　1/16　　印张：21.25　　字数：494 千
印　　数：3 000 册
书　　号：ISBN 978-7-113-11394-0
定　　价：55.00 元（附赠光盘）

前言 Foreword

对于网络安全工作者来讲，了解黑客编程的原理对有效地抵御黑客的攻击极为有用。实际上，黑客编程与普通的编程并无多大区别，只是侧重的方向不太相同。本书对目前流行的一些黑客编程技术逐一进行讲解，揭开黑客编程的神秘面纱。

本书的内容安排

全书共包含 15 章，其中第 1 章和第 2 章为本书的基础入门篇，第 3～9 章为全书重点，详细介绍了目前流行的各种黑客技术编程，第 10～15 章为一些常见的安全防御编程和部分高级内容。

各章节内容简介如下：

章　节	章　节　内　容
第 1 章	主要对本书内容进行简单的介绍，以及一些注意事项，并通过两个简单的例子介绍了本书所用开发平台的使用方法，为全书的基础
第 2 章	使用 VC 和 BCB 通过两个简单小程序对 Windows 编程的基础操作——文件操作技术进行了详细的介绍，使读者详细领会 VC 和 BCB 这两款工具的使用方法
第 3 章	使读者对曾经让人闻之色变的病毒编程技术有全面的认识，能够理解病毒的工作原理并进行针对性防御
第 4 章	详细地分析了一个简单后门所具备的基本功能实现，如自启动、屏幕监控、系统控制、反弹后门等技术
第 5 章	通过一个简单的端口扫描器带领读者学习多线程、原始套接字等部分高级的编程技巧，同时也对 WinPcap 进行了简单介绍，详细讲述了 Sniffer（即嗅探器）的编程原理
第 6 章	在介绍木马下载者的编写过程中使读者学习到 WinInet 编程、服务端生成技术、UPX 加壳技术等有趣的内容
第 7 章	通过一个 U 盘小偷示例使读者深入理解 Windows 的消息工作机制
第 8 章	介绍密码大盗与键盘记录器的编写原理及防御方法，也介绍 ASP 收信、邮箱收信等编程技巧
第 9 章	对一些常见的验证码格式进行了详细分析，并通过一个实例使读者了解这个此前并不算流行的领域
第 10 章	综合介绍了进程创建、进程枚举、进程隐藏以及进程保护等多项内容
第 11 章	以“熊猫烧香”病毒为例介绍了如何通过对病毒进行分析编写出一个简易的病毒专杀工具，简单介绍了 PE 文件格式

续表

章　节	章　节　内　容
第 12 章	全面介绍了 NTFS 数据流，学会编程对其进行检测和清除
第 13 章	介绍了文件、注册表、进程等几种常见的监控技术
第 14 章	介绍了目前十分流行的 API Hook 及 SPI 编程技术
第 15 章	介绍了 WinLogon 通知包的编程方法，以及在安全编程中经常遇到的 SSDT 挂钩和恢复方法

本书适合读者

本书适合 Windows 编程爱好者、熟悉 Windows 操作系统的计算机安全从业人员、刚刚学会 C/C++语言并亲自编写过一些小型程序的读者。

由于本书涉及一些 Windows 可视化程序设计，因此希望读者最好能有一些使用 Visual C++或 C++ Builder 进行 Windows 程序设计的经验，这样将更有助于您深入地理解本书所讲述的内容。

本书声明

本书中的代码仅供编程学习和测试之用，请勿将其用于非法目的，否则后果自负。编程是一种乐趣，但把编程用来进行破坏则是违法行为！

由于笔者能力所限，书中不足之处在所难免，还望读者批评指正。

本书为避免代码用于非正当用途，不在随书光盘中提供完整源代码，对本书有所建议，请直接与作者本人联系，联系方式如下：

邮件：peiyaoqiang@126.com 或 wwb_beijing@163.com

编　者

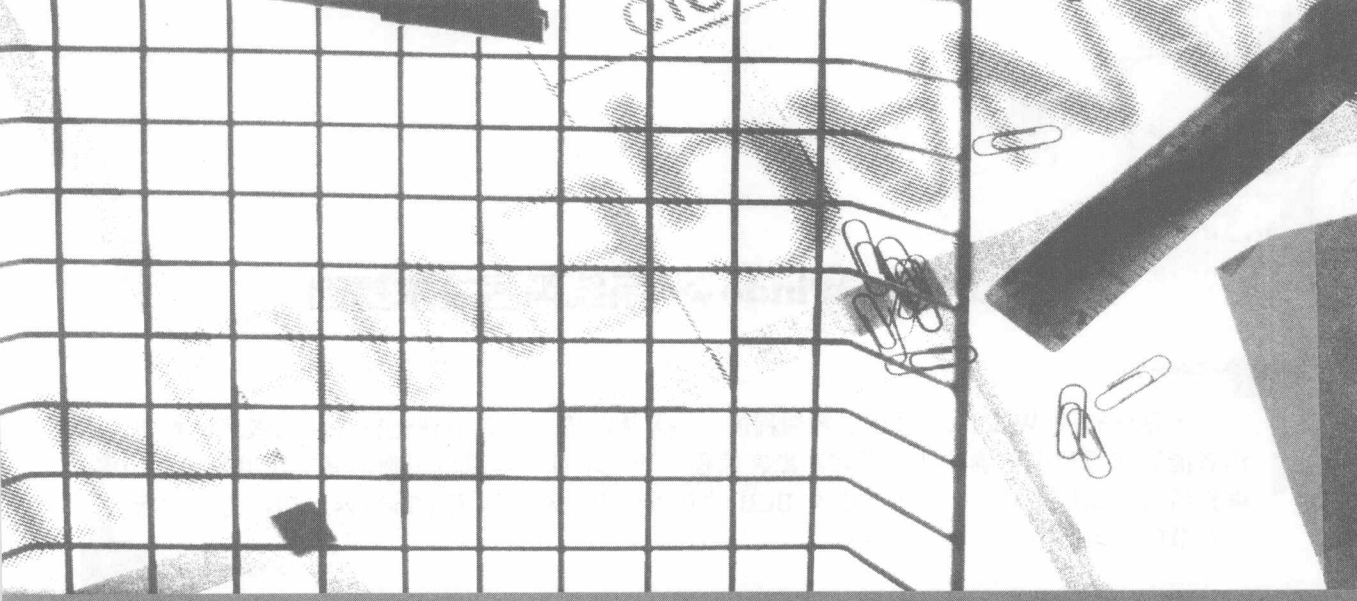
2010 年 4 月

目录 Contents

第 1 篇　Windows 系统黑客技术基础入门

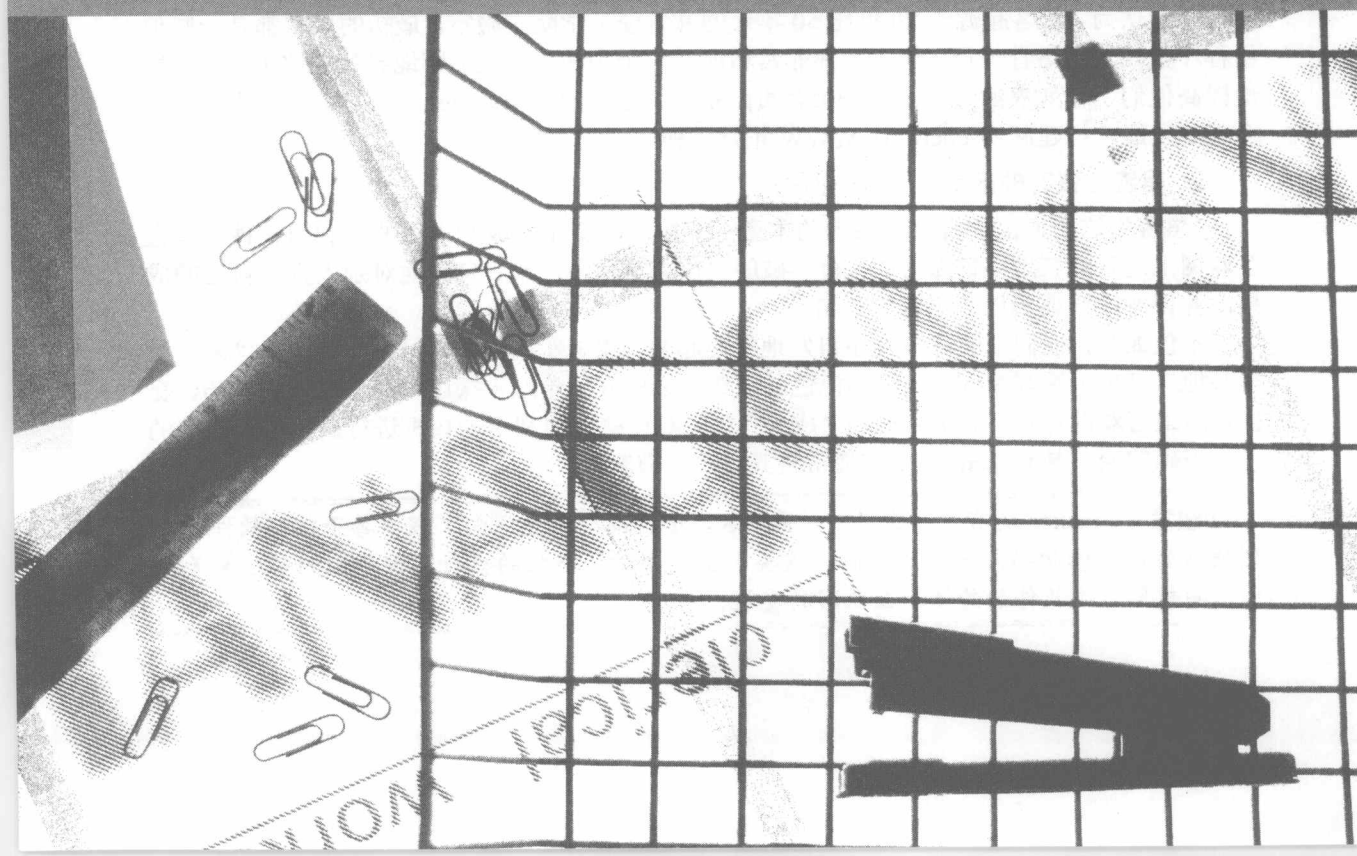
第 2 篇 黑客技术编程

第 3 篇 安全防御



第 1 篇

Windows 系统黑客技术基础入门



第 1 章　Windows 系统黑客技术基础

本章就有关 Windows 系统黑客编程的一些基本概念和学习方法进行简要的叙述，希望读者能够在思想上正确地认识黑客和黑客编程。通过本章的学习，明确本书所使用的平台、编程语言、编程工具等，了解 VC 与 BCB 的基本使用方法，认识 Windows API，为本书后续章节的学习打下一个坚实的基础。

1.1　认识黑客编程

本节作为全书的开篇，将向读者解释什么是黑客，黑客编程究竟有什么特殊之处，怎样才能快速了解、掌握、剖析黑客编程等关键性的问题。俗话说“磨刀不误砍柴工”，虽然本节没有讲解任何立竿见影的技术，但笔者还是希望读者能够认真地阅读。

1.1.1　什么是黑客

“黑客”源自英文单词 hacker，主要是指专门研究、发现计算机和网络漏洞的计算机爱好者。

1. 黑客的起源

一般认为，黑客起源于 20 世纪 50 年代的麻省理工学院实验室。最初的黑客都是一些顶级程序员或者网络管理员，他们大都非常精通某一个领域，并且不懈地寻找能够更快、更好地提高他们工作效率的方法。这些黑客贡献很大，他们建起 Internet，使 UNIX 操作系统有今天的发展，搭建起 Usenet，让 WWW 正常运转。

2. 黑客与骇客的区别

“黑客”这个词语的含义与最初的本意有了极大的变化，成千上万的人利用各种工具在互联网上进行疯狂地盗窃账号、入侵、破解、攻击等行为，然后自豪地对别人宣传自己的成果，并得意洋洋地冠以“黑客”之名。

不仅如此，他们中的许多人还自发地纠集起来，组成了诸如“××黑客联盟”、“××黑客基地”、“××黑客领域”等形形色色的组织，并成立了论坛，探讨交流一些入侵技巧，交换各自最喜欢的工具，炫耀自己的“成果”等。对这些专门利用计算机进行破坏或恶作剧的人，正确的叫法是 Cracker，中文通常将其译为“骇客”。

> 注意：Cracker 还有一种含义——破解者，专指那些熟悉逆向工程，善于破解软件以达到使其验证或保护功能失效的目的。这类人虽然推动了盗版的盛行，但他们的做法毫无疑问，同样促进了软件的传播和互联网的发展。

3. “黑客”的本质

黑客的本质没有改变，他们热衷于发现和修补漏洞，改善网络中存在的缺陷等。曾经有人说过，“黑客存在的意义就是使网络变得更加安全完善”。可用一句话来准确地揭示出黑客与骇客的区别：黑客是在建设，而骇客是在破坏。

1.1.2　了解黑客编程

编程是每一个黑客理应具备的基本技能。最早的黑客本来就是一些优秀而又不满足于现状的顶级程序员，但黑客又往往与普通的程序员不同。

1. 普通程序员与黑客的区别

对于普通的程序员来讲，他们的编程任务就是根据需求用最正规的方法实现程序，通常初级程序员很少考虑程序的效率、安全性等问题，更不会费尽心思揣摩某个功能的底层实现方法。举例来说，一般的 Windows 程序员都会熟练地使用 Win32 API 实现一些常见的程序，但他们大多不会考虑这些 Win32 API 的底层实现细节，也很少考虑到程序的安全性。

而黑客却不同，他们喜欢追求掌握一门语言的精髓，对各种函数的底层实现细节非常热衷；他们编写程序非常注重安全性，能够考虑到许多正规程序员不会想到的地方；他们在使用其他人编写的程序时往往不会安分，而是经常试图通过各种方法找出这些软件中可能存在的漏洞，然后将其公布并通知软件的官方处理。

2. 黑客编程与其他编程的区别

单纯从编程的过程来看，黑客编程与其他编程并无本质上的区别，如果非要总结出几点，黑客编程比较侧重对系统的控制、优异的执行效率和稳定性、安全性等。因此，学习黑客编程对自身的知识深度和宽度要求较高，例如对操作系统的深入理解、高效率算法的设计等。

3. 黑客编程的内容

黑客编程的内容极为广泛，基本上所有编程方向都可以为黑客编程起到补充作用。常见的系统及内核编程自不必说，就连人们通常以为与黑客无关的编程技术实际上也总是与黑客编程密切相关。黑客编程最有代表性的两点：

- 操作系统；
- 网络编程。

操作系统是各种程序赖以运行的平台，在编写程序时也在使用操作系统提供的开发接口，黑客通过对操作系统的深入学习，能够使编程水平大大提高。互联网就是黑客大展身手的舞台，不懂得网络编程简直是一件令人无法想象的事情。

1.2　选择操作系统和编程语言

1.2.1　本书应用的操作系统

本书中的所有操作均在 Windows 系统平台下进行，并且如无特殊说明，本书中所涉及