

赠

CD多媒体光盘

赠送作者编写的部分代码和工具

Windows
网络安全技术专家
倾力巨献

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

特邀编辑: 王 惠

封面设计: 张 丽

责任印制: 李 佳

读者热线电话: 400-668-0820

封面制作: 白 雪

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)



版权所有 侵权必究

凡购买铁道版图书,如有印制质量问题,请与本社计算机图书批销部联系调换。

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 ww_beiing@163.com

编 者

2010 年 4 月

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	2
1.1 认识黑客编程	2
1.1.1 什么是黑客	2
1.1.2 了解黑客编程	3
1.2 选择操作系统和编程语言	3
1.2.1 本书应用的操作系统	3
1.2.2 本书选择的编程语言	4
1.3 本书选择的开发工具	4
1.3.1 Visual C++ 6.0 的使用方法	5
1.3.2 Borland C++ Builder 6 的使用方法	8
1.4 认识 Windows API	11
1.4.1 API 与可视化编程环境	11
1.4.2 C 语言标准库函数和 API 函数的区别	12
1.4.3 具有字符串参数的 API 函数	12
第 2 章 文件操作技术	14
2.1 使用 C 语言标准库函数进行文件操作	14
2.1.1 打开文件	14
2.1.2 关闭文件	15
2.1.3 读文件	15
2.1.4 写文件	16
2.1.5 文件定位	16
2.2 使用 Windows API 函数进行文件操作	17
2.2.1 CreateFile() 函数	17
2.2.2 CloseHandle() 函数	18
2.2.3 ReadFile() 函数	19
2.2.4 WriteFile() 函数	19
2.2.5 SetFilePointer() 函数	19
2.2.6 DeleteFile() 函数	20
2.2.7 CreateDirectory() 函数	20

2.2.8	RemoveDirectory()函数	21
2.2.9	CopyFile()函数	21
2.2.10	MoveFile()函数	21
2.2.11	GetFileAttributes()函数和 SetFileAttributes()函数	21
2.3	文本加密器	23
2.3.1	文本加密的原理	23
2.3.2	使用 VC 实现文本加密器	24
2.4	文件粉碎机	25
2.4.1	Windows 删除文件的原理	25
2.4.2	使用 BCB 实现文件粉碎	26

第 2 篇 黑客技术编程

第 3 章 计算机病毒的基本原理与防御.....30

3.1	计算机病毒概述	30
3.1.1	什么是病毒	30
3.1.2	病毒编程技术说明	31
3.2	注册表编程	31
3.2.1	认识注册表	31
3.2.2	注册表编程技术	32
3.3	自删除技术的模拟	36
3.3.1	自删除技术简介	37
3.3.2	自删除技术的 3 种方式	37
3.3.3	自删除技术应用	38
3.4	剖析映像劫持技术	39
3.4.1	什么是映像劫持	39
3.4.2	映像劫持详细分析	40
3.4.3	防范映像劫持技术攻击	42
3.5	彻底认识 Autorun.inf 文件	43
3.5.1	Autofun.inf 文件简介	43
3.5.2	Autofun.inf 文件参数	43
3.6	病毒实现典型代码分析	44
3.6.1	隐藏运行, 将自身移动到系统目录	45
3.6.2	修改注册表相关键值	45
3.6.3	遍历所有硬盘生成 Autorun.inf 文件	46
3.7	病毒的查杀与防御	46
3.7.1	病毒的查杀与防御简介	47
3.7.2	防火墙主动防御设置	47

第 4 章 后门编程与防御技术	49
4.1 后门概述	49
4.2 Winsock 网络编程基础	50
4.2.1 C/S 模式	50
4.2.2 Winsock API 及其常用函数简介	50
4.3 后门分析之自启动	56
4.3.1 启动文件夹	56
4.3.2 自身复制程序	57
4.3.3 注册表启动键值	58
4.3.4 应用程序关联	58
4.3.5 启动文件	59
4.4 Windows 服务编程技术	59
4.4.1 Windows 服务	60
4.4.2 编写服务程序	60
4.5 服务控制编程技术	62
4.5.1 打开 SCM——OpenSCManager()函数	63
4.5.2 打开一个服务对象——OpenService()函数	63
4.5.3 安装一个服务——CreateService()函数	63
4.5.4 启动一个服务——StartService()函数	64
4.5.5 查询服务的运行状态——QueryServiceStatus()函数	64
4.5.6 控制操作——ControlService()函数	65
4.5.7 删除服务——DeleteService()函数	65
4.6 后门分析之屏幕截取	66
4.6.1 屏幕截取简介	66
4.6.2 MFC 类实现屏幕截取	66
4.6.3 BCB 实现屏幕截取	68
4.7 后门分析之系统信息搜集与控制	69
4.7.1 关闭/重启计算机	69
4.7.2 指定 HTTP 地址下载文件	70
4.7.3 清除系统日志	71
4.8 后门分析之结果回显	72
4.8.1 管道后门简介	72
4.8.2 双管道后门代码	72
4.9 透视后门连接机制	73
4.10 后门的查杀与防范	74
4.10.1 怀疑被感染	74
4.10.2 确定被感染	76
4.10.3 手动杀毒	76

第 5 章 扫描嗅探技术原理剖析.....	79
5.1 认识多线程.....	79
5.1.1 理解线程	79
5.1.2 利用标准 Windows API 创建多线程程序	80
5.1.3 利用 BCB 提供的线程类.....	83
5.2 网络编程深入之原始套接字.....	84
5.2.1 原始套接字简介.....	84
5.2.2 利用原始套接字嗅探数据流.....	85
5.3 扫描的实现.....	87
5.3.1 完整端口扫描.....	87
5.3.2 TCP SYN 扫描	91
5.4 使用 WinPcap	96
5.5 Sniffer 原理剖析.....	99
5.5.1 Sniffer 的危害	100
5.5.2 Sniffer 的工作原理.....	100
5.5.3 TCP/IP 协议的 4 层结构.....	101
5.6 Sniffer 编程实现.....	103
5.7 ARP 欺骗.....	106
5.7.1 ARP 欺骗简介.....	106
5.7.2 ARP 欺骗演示程序.....	106
5.8 针对扫描嗅探的防御.....	108
5.8.1 针对扫描的防御.....	108
5.8.2 针对嗅探的防御.....	109
5.8.3 针对 ARP 欺骗的防御.....	110
第 6 章 木马下载者的技术分析与防范.....	111
6.1 认识木马下载者.....	111
6.1.1 “挂马”原理.....	111
6.1.2 木马下载者简介.....	112
6.2 网络编程深入之 WinInet.....	112
6.2.1 InternetOpen()函数.....	112
6.2.2 InternetConnect()函数	113
6.2.3 InternetOpenUrl()函数	114
6.2.4 InternetQueryDataAvailable()函数.....	115
6.2.5 InternetReadFile()函数	115
6.2.6 InternetSetFilePointer()函数.....	116
6.2.7 InternetWriteFile()函数	116
6.2.8 InternetCloseHandle()函数.....	117

6.2.9	WinInet 下载程序演示	117
6.3	服务端生成技术	121
6.3.1	FindResource()函数	121
6.3.2	LoadResource()函数	122
6.3.3	SizeofResource()函数	122
6.3.4	LockResource()函数	122
6.3.5	服务器端程序演示	123
6.4	UPX 加壳技术	126
6.4.1	UPX 加壳技术简介	126
6.4.2	UPX 加壳技术演示	126
6.5	木马下载者的防御	127
6.5.1	配置防火墙	127
6.5.2	更新系统	128
第 7 章	U 盘小偷的剖析与防御	129
7.1	认识 U 盘小偷	129
7.1.1	U 盘小偷概述	129
7.1.2	U 盘查找的简单实现	130
7.2	理解 Windows 消息机制	130
7.2.1	消息的基本概念	130
7.2.2	Windows 消息系统	131
7.2.3	SDK 消息机制	132
7.2.4	BCB 消息机制	132
7.2.5	非标准消息	136
7.2.6	自己发送消息	137
7.3	U 盘小偷的原理	138
7.3.1	关于事件	139
7.3.2	捕获 U 盘事件	139
7.4	全局热键的实现	144
7.4.1	GlobalAddAtom()函数	144
7.4.2	RegisterHotKey()函数	145
7.4.3	UnregisterHotKey()函数	145
7.5	防御 U 盘小偷	146
7.5.1	防御 U 盘小偷的原理	146
7.5.2	加密 U 盘	146
7.5.3	解密 U 盘	148
7.6	其他编程技巧分析	149
7.6.1	通过 INI 文件保存配置信息	149
7.6.2	U 盘防火墙	150
7.6.3	只允许运行一个实例	151

7.6.4 遍历搜索指定的文件类型	151
7.6.5 添加作者主页链接	152
7.6.6 显示版权信息对话框	153

第 8 章 密码盗窃的模拟与防范

154

8.1 密码大盗与键盘记录器简介	154
8.1.1 密码大盗简介	154
8.1.2 键盘记录器简介	156
8.2 密码大盗工作原理与功能模拟	156
8.2.1 密码大盗工作原理	156
8.2.2 密码大盗功能演示	156
8.2.3 密码大盗功能实现	157
8.3 键盘记录器工作原理与功能模拟	161
8.3.1 键盘记录器工作原理	161
8.3.2 钩子简介	162
8.3.3 使用钩子实现键盘记录器	164
8.4 ASP 收信的实现	167
8.4.1 ASP 收信简介	167
8.4.2 ASP 收信程序解析	167
8.5 邮箱收信的实现	169
8.5.1 邮箱收信简介	169
8.5.2 邮箱收信程序解析	169
8.6 密码大盗与键盘记录器的防御与查杀	171
8.6.1 使用反病毒软件	171
8.6.2 使用主动反击法	171

第 9 章 验证码的破解与防范

173

9.1 认识验证码	173
9.1.1 验证码的起源	173
9.1.2 验证码的工作原理	173
9.1.3 验证码的分类	174
9.1.4 破解验证码的原理分析	174
9.2 BMP 文件结构分析	177
9.2.1 BMP 文件结构概述	177
9.2.2 BMP 文件头信息	178
9.2.3 BMP 图像信息	180
9.3 分析 Z-Blog 验证码	183
9.3.1 什么是 OCR	183
9.3.2 分析 Z-Blog 验证码	184

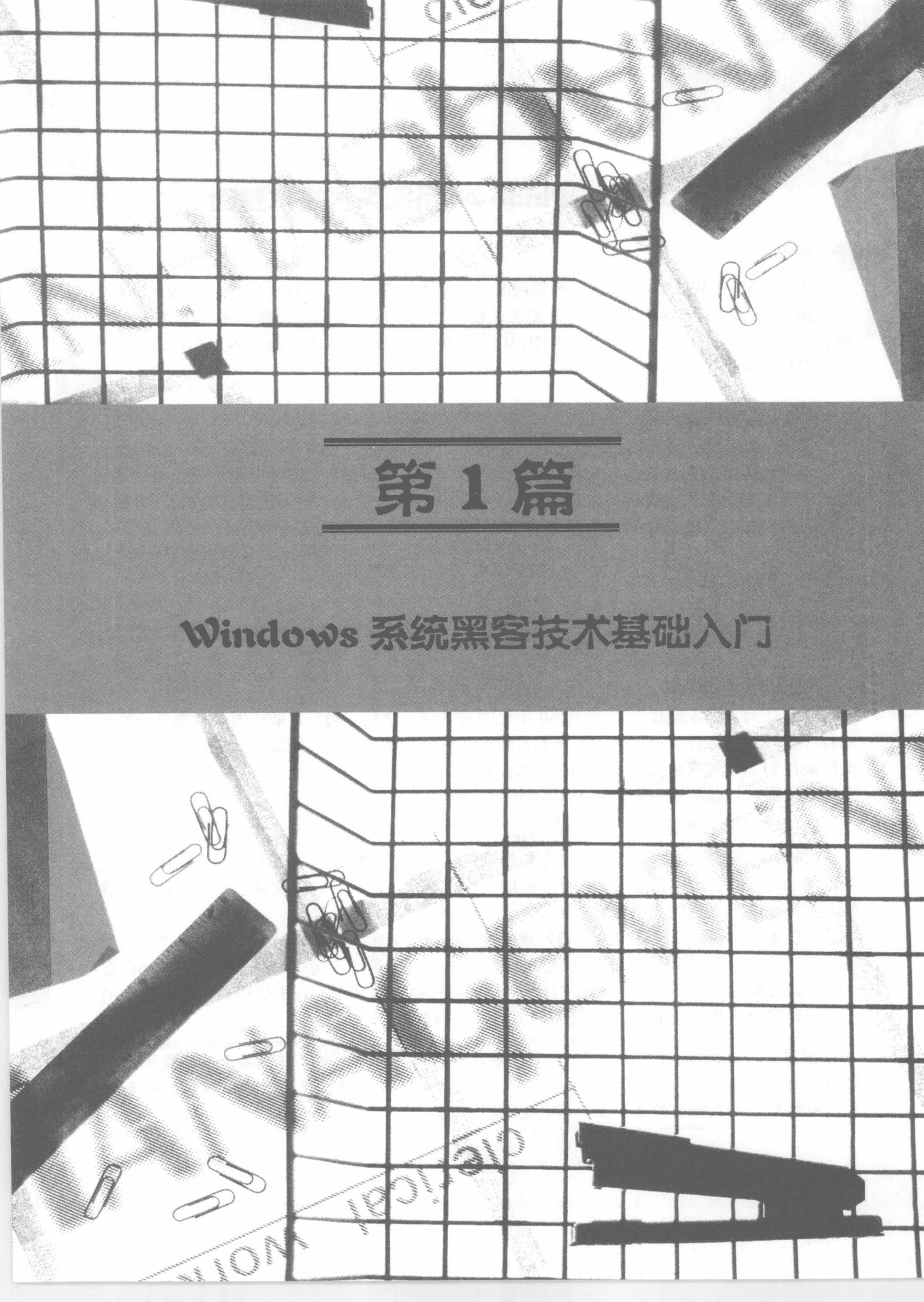
9.4	Z-Blog 验证码的破解原理分析	185
9.4.1	将验证码图片下载到本地	185
9.4.2	将验证码加载到程序的相应位置	186
9.4.3	分析验证码图片	186
9.5	验证码破解攻击的防范方法	189

第 3 篇 安全防御

第 10 章	进程控制技术	191
10.1	进程概述	191
10.2	进程的创建	192
10.2.1	WinExec() 函数	192
10.2.2	ShellExecute() 函数	192
10.2.3	CreateProcess() 函数	194
10.3	进程的管理与控制	195
10.3.1	打开进程	195
10.3.2	操作进程权限	195
10.3.3	终止进程	196
10.4	动态链接库编程	197
10.4.1	动态链接库的创建	197
10.4.2	动态链接库的调用	199
10.5	进程的枚举	200
10.5.1	系统快照	200
10.5.2	利用 PSAPI	201
10.5.3	利用 WTSAPI	202
10.5.4	利用 NTDLL	203
10.6	进程的隐藏	204
10.6.1	进程隐藏简介	204
10.6.2	进程隐藏方法	205
10.7	进程保护技术	209
第 11 章	病毒专杀工具的编写	210
11.1	“熊猫烧香”病毒及专杀工具分析	210
11.1.1	“熊猫烧香”病毒与其感染特征	210
11.1.2	“熊猫烧香”病毒专杀工具工作流程	211
11.2	PE 文件格式分析	211
11.2.1	PE 文件格式整体概要	211
11.2.2	DOS MZ header 分析	212
11.2.3	PE header 分析	212

11.2.4	IMAGE_OPTIONAL_HEADER 分析	212
11.2.5	IMAGE_SECTION_HEADER 分析	214
11.2.6	PE 文件格式分析程序示例	214
11.2.7	PE 文件感染分析	217
11.3	“熊猫烧香”病毒专杀工具的主要代码	217
11.3.1	启动专杀工具	217
11.3.2	扫描进程	219
11.3.3	扫描 aurorun.inf	220
11.3.4	查找并恢复感染文件	221
11.3.5	主函数	222
11.4	清除感染痕迹	223
11.4.1	修改图标	223
11.4.2	清除注册表项和值	223
11.5	免疫功能实现	226
第 12 章	NTFS 数据流的检测与清除	231
12.1	认识 NTFS 数据流	231
12.1.1	数据流的概念演示	231
12.1.2	数据流特性演示	232
12.1.3	NTFS 数据流的读/写	233
12.2	NTFS 数据流的深入分析	233
12.2.1	利用 WinRar 实现隐藏文件	234
12.2.2	利用 ScanNTFS 查找和清除 NTFS 数据流	235
12.3	NTFS 数据流扫描器的实现	236
12.3.1	数据流扫描器原理	236
12.3.2	main()函数	237
12.3.3	FindAllFilesInDirectory()函数	238
12.3.4	GetFileDataStream()函数	240
12.3.5	ReadStream()函数	240
第 13 章	系统监控技术	243
13.1	系统监控概述	243
13.2	文件监控技术	243
13.2.1	使用 FindChangeNotification 系列函数	243
13.2.2	使用 ReadDirectoryChangesW()函数	246
13.3	注册表监控技术	249
13.3.1	RegNotifyChangeKeyValue()函数简介	249
13.3.2	RegNotifyChangeKeyValue()函数使用演示	249
13.4	进程监控技术	251

13.4.1	shell 钩子简介	251
13.4.2	创建 shell 钩子	252
第 14 章	API Hook 与 SPI	257
14.1	API Hook 综述	257
14.1.1	代理 DLL	257
14.1.2	磁盘文件补丁	258
14.1.3	内存补丁	258
14.2	API Hook 实例	258
14.2.1	API Hook 的编写	258
14.2.2	API Hook 的测试	263
14.3	使用 Detours 实现 API Hook	265
14.4	SPI 综述	266
14.4.1	SPI 简介	266
14.4.2	LSP 的安装	267
14.5	SPI 实例	272
14.5.1	SPI 的编写	272
14.5.2	SPI 的测试	288
第 15 章	WinLogon 编程和 SSDT 的挂钩与恢复	290
15.1	WinLogon 概述	290
15.2	WinLogon 编程实例	291
15.3	认识 SSDT	293
15.4	挂钩 SSDT	294
15.5	恢复 SSDT	298
15.5.1	获取系统服务函数原始地址	299
15.5.2	恢复 SSDT 的实现代码	301
15.5.3	应用层实现代码	311
附录 A	Visual C++ 6.0 的安装	315
附录 B	Borland C++ Builder 6.0 的安装	320

The background of the entire page is a complex artistic composition. It features a prominent grid pattern, likely from a piece of graph paper, which is partially obscured by various objects. Several paper clips are scattered across the grid, some attached to it and others lying on the surface. A ruler is visible in the upper right and lower left areas. The overall aesthetic is technical and precise, reflecting the book's theme of system hacking.

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