

网管员典藏书架

WANG GUAN YUAN DIAN CANG SHU JIA

HACKERS
PROGRAMMING

彻底研究

黑客编程技术揭秘

与 攻防实战

赵笑声◎编著

基于网络安全，登堂入室
定制属于自己的黑客攻防软件

知己知彼，完整再现黑客主流攻击实现方式和攻防案例，提升实战技能

细致入门和最佳实践相辅相成

为网管员典藏书架再添宝典

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE



HACKERS
PROGRAMMING

彻底研究
黑客编程技术揭秘
与
攻防实战

赵笑声◎编著

内 容 简 介

本书全面介绍了在 Windows 环境下使用 Socket API 开发各类黑客软件及系统安全防护工具软件的编程实现方法。

在讲解细节上,本书循序渐进地向读者介绍了黑客攻击程序、安全防护工具、远程控制软件、网络安全管理软件的原理及具体编程实现方法,从当前热门的黑客软件和安全防护工具中选择典型案例,深入分析。

本书不仅适用于黑客程序开发,在读者掌握本书介绍的各种编程技术后还能胜任开发各类网络安全防护软件,是读者成为专业的网络开发工程师不可不读的书籍。

图书在版编目(CIP)数据

彻底研究 : 黑客编程技术揭秘与攻防实战 / 赵笑声
编著. —北京: 中国铁道出版社, 2016. 8
ISBN 978-7-113-21986-4

I. ①彻… II. ①赵… III. ①C 语言—程序设计
IV. ①TP312

中国版本图书馆 CIP 数据核字 (2016) 第 146060 号

书 名: 彻底研究: 黑客编程技术揭秘与攻防实战
作 者: 赵笑声 编著

责任编辑: 荆 波
责任印制: 赵星辰

读者热线电话: 010-63560056
封面设计: **MXK** DESIGN
STUDIO

出版发行: 中国铁道出版社(北京市西城区右安门西街8号 邮政编码: 100054)
印 刷: 北京明恒达印务有限公司
版 次: 2016年8月第1版 2016年8月第1次印刷
开 本: 787mm×1092mm 1/16 印张: 32.5 字数: 719千
书 号: ISBN 978-7-113-21986-4
定 价: 69.80元

版权所有 侵权必究

凡购买铁道版图书,如有印制质量问题,请与本社读者服务部联系调换。电话:(010) 51873174

打击盗版举报电话:(010) 51873659

前 言

对专业人士来说，“黑客”并不神秘。黑客技术也只是计算机安全技术分支之一，也是有章可循的。有人利用黑客技术做“小偷”类违法犯罪的事情，我们需要培养出技术更强、训练有素的“警察”即可。本书就是这样一本希望通过揭秘网络底层开发技术，培养出更多更优秀的系统、网络安全软件开发者的。

“能编写出属于自己的黑客软件”一直是很多网络安全爱好者梦寐以求的。为了让更多的网络安全爱好者能够迅速掌握黑客软件、安全工具的开发技术，也为了提高国内网络安全技术的整体水平，笔者精心编写了本书。

笔者根据自己多年的学习和工作经验，结合当前网络安全技术最新的发展态势，循序渐进地为读者讲解如何在 Visual C++ 环境下开发各种黑客工具和安全软件。本书旨在技术上为读者提供一个学习的方法和参考，其中部分技术可能存在一定的破坏性，需要读者在学习时慎重使用并用于合适的测试环境。本书以实例开发了安全软件的雏形，源代码发布在出版社网站上，请读者移步下载，或者到 QQ 学习交流群 82481994 中下载。

本书的内容安排

本书共分为三篇，共 15 章，以网络编程最基本的 Windows Sockets API 开始，逐步介绍简单的网络扫描器技术，让读者轻松入门。通过常见黑客工具及下载者程序的编写和防范，让读者对编程技术有一个更大的提高。在读者掌握了一定的黑客软件开发基础后，笔者开始介绍 Rootkit 编程技术及远程控制技术，让读者通过一个完整综合的实例学习 Visual C++ 开发黑客软件。最后结合笔者的工作经验介绍了网络准入技术和网络蜘蛛等拓展技术，供有兴趣的读者深入学习。

第一篇（第 1~3 章）：初入门径

讲述了使用 Visual C++ 开发黑客软件，尤其是基于网络的黑客软件必须具备的理论基础及入门级的编程实例。通过本章学习，读者可以掌握 Windows Sockets API 编程开发的技术、网络扫描程序及认证程序破解的编程实现，从而为进一步提高编程水平打下基础。

第二篇（第 4~7 章）：做一个专业的黑客

讲述了拒绝服务攻击技术的原理及实现，感染型下载者程序的功能、原理及编程实现，Rootkit 技术的编程实现。通过本章学习，读者的黑客编程技术将得到很大提高。本章介绍的 3 类典型程序是当前互联网最为流行的黑客攻击技术或实现方式。同时针对下载者程序，笔者还讲解了如何有针对性地防范，并通过 U 盘病毒防火墙的形式予以实现。

第三篇（第 8~15 章）：成为大师的修炼

本篇通过一个完整的黑客软件——“远程控制软件”的功能、原理、设计、实现及优化等方

面，为读者深入剖析了一个完整黑客软件的开发流程。本篇是前几章编程技术的综合，是各种技术的综合运用。笔者在本篇详细地介绍了编程中的各个细节，同时首次公开了部分远程控制软件的关键代码。并且结合笔者的工作和学习经验，介绍了网络准入技术、网络蜘蛛、SSDT 恢复等技术的原理及实现方式。对于希望进一步提高自己黑客软件开发技术的读者无疑是一个拓展机会。通过学习本篇，为读者将来开发出自己的网络安全工具或软件提供了必要的铺垫作用。

本书的特点

从 Windows Sockets API 编程基础到最基本的网络扫描器编程，从基本黑客攻击程序到基于认证的网络程序破解，从流行下载者程序的编程实现到 U 盘防火墙等安全工具，从 Windows 底层的 Rootkit 编程到远程控制软件开发，从网络准入控制结束到网络蜘蛛等，本书逐个讲解各类黑客软件的实现原理，并通过代码编程实现，其中很多代码尚属首次公开。

本书的特点主要体现在以下几个方面：

- 本书的编排采用循序渐进的方式，适合对 Visual C++ 程序开发有一定了解，并对黑客程序开发抱有极大兴趣的网络安全爱好者。
- 本书结合笔者多年的工作和学习经验积累，通过对流行网络安全技术中典型案例的编程实现，为读者提供了快速学习和进步的参考。
- 本书在介绍大量网络安全技术实现原理时，都提供了典型的案例和参考的图例。读者通过对原理的学习，能够掌握 Visual C++ 开发黑客工具的具体技术，同时也能更加深入地理解网络安全技术的具体细节，从而提高自身的技术水平。
- 本书除了介绍主流的安全技术及编程方法，还涉及 Rootkit、SSDT 恢复等系统底层编程技术，对于希望提高黑客软件开发技术的读者无疑是一个很大的帮助。
- 本书突破常规，对重要的编程技术和细节没有遮遮掩掩，其中部分功能实现的代码尚属首次公开。当然，为了防止一些具有破坏性的程序被错误使用造成不必要的破坏，笔者对光盘中的部分代码做了技术处理，相信有一定编程基础的读者能够自行解决。
- 本书虽然以黑客软件开发为基本出发点，但是又不仅限于黑客技术；笔者更多的是从技术角度探讨技术原理及实现方法，同时将网络安全思想时刻灌注其中。书中涉及的 U 盘防火墙、网络准入技术等都是笔者对当前互联网黑客攻击泛滥的思考和防范方法的具体实现。

适合阅读本书的读者

本书由河南城建学院的赵笑声编写。全书由浅入深，由理论到实践，尤其适合对 Visual C++ 环境有一定了解，同时对黑客软件开发抱有极大兴趣的初级读者学习并逐步完善自己的知识结构。具体来说，以下读者应该仔细阅读本书：

- 希望进入应用软件开发行业的新手。
- 迫切希望提高个人开发测试技能和水平的初级程序测试人员。
- 具备一定的研发理论知识但是缺乏实践的软件研发工程师。
- 希望了解国内外黑客软件开发的动向以及最新反黑客软件的开发人员。

作者

2016年5月

目 录

第 1 章 黑客入门, Socket API 开发必知	1
1.1 Windows API 和 Socket	1
1.1.1 Windows API 编程的优点	1
1.1.2 Socket 通信流程	2
1.2 服务器端 Socket 的操作	3
1.2.1 在初始化阶段调用 WSASocket	3
1.2.2 建立 Socket	4
1.2.3 绑定端口	4
实例 1.1 bind 函数调用示例	5
1.2.4 监听端口	6
1.2.5 accept 函数	6
实例 1.2 accept 函数示例	7
1.2.6 WSASocket 函数	7
实例 1.3 响应 Socket 事件的结构代码	8
1.2.7 结束服务器端与客户端 Socket 连接	8
1.3 客户端 Socket 的操作	9
1.3.1 建立客户端的 Socket	9
1.3.2 发起连接申请	9
实例 1.4 connect 函数示例	9
1.4 Socket 数据的传送	9
1.4.1 TCP Socket 与 UDP Socket	10
1.4.2 发送和接收数据的函数	10
1.5 自定义 CMyTcpTran 通信类	12
1.5.1 为什么要使用类	13
1.5.2 Visual C++ 中创建通信类	13
实例 1.5 CMyTcpTran 类头文件	15
1.5.3 CMyTcpTran 类的代码实现	17

实例 1.6	CMyTcpTran 类方法的函数实现.....	17
实例 1.7	Socket 通信库初始化实现方法.....	18
实例 1.8	初始化套接字资源.....	18
实例 1.9	创建连接通信函数的实现.....	20
实例 1.10	初始化 Socket 资源的接收函数.....	21
实例 1.11	发送套接字数据的函数实现.....	23
1.6	小结	25
第 2 章	专业风范，网络扫描器的开发实现.....	26
2.1	扫描器的产生及原理.....	26
2.1.1	扫描器的产生	26
2.1.2	不同扫描方式扫描器原理及性能简介	27
2.2	主机扫描技术	29
2.2.1	ICMP Echo 扫描.....	29
2.2.2	ARP 扫描	30
2.3	端口扫描技术	31
2.3.1	常用端口简介	31
2.3.2	TCP connect 扫描.....	32
2.3.3	TCP SYN 扫描	33
2.4	操作系统识别技术.....	33
2.4.1	根据 ICMP 协议的应用得到 TTL 值	33
2.4.2	获取应用程序标识.....	35
2.4.3	利用 TCP/IP 协议栈指纹鉴别	35
2.4.4	操作系统指纹识别依据	36
2.4.5	操作系统指纹识别代码实现.....	39
2.4.6	Web 站点猜测	48
2.4.7	综合分析	49
实例 2.1	一段端口检测程序代码.....	50
2.5	扫描器程序实现	52
2.5.1	ICMP echo 扫描原理.....	52
2.5.2	ICMP echo 扫描的实现方法	53
实例 2.2	ICMP 扫描程序类定义.....	54
实例 2.3	ICMP 扫描的代码实现.....	55
实例 2.4	ICMP 扫描判断主机存活	58
2.5.3	ARP 扫描的原理.....	59
2.5.4	ARP 扫描的实现方法	60

实例 2.5 ARP 设备扫描的实现方式.....	60
实例 2.6 ARP 扫描程序实例.....	64
2.5.5 TCP SYN 扫描的原理.....	66
2.5.6 TCP SYN 扫描的实现方法.....	66
实例 2.7 TCP SYN 扫描实例.....	66
2.5.7 综合应用实例——ARP 欺骗程序.....	70
2.5.8 ARP 欺骗的原理.....	70
2.5.9 Winpcap 环境初始化.....	70
实例 2.8 Winpcap 驱动程序初始化.....	70
2.5.10 欺骗主程序.....	77
实例 2.9 ARP 欺骗程序的实现方法.....	77
2.6 资产信息扫描器开发.....	83
2.6.1 资产信息扫描器的应用范围.....	83
2.6.2 snmp 协议扫描的原理.....	84
2.6.3 snmp 协议扫描的实现方法.....	84
实例 2.10 snmp 协议扫描的实现方法.....	84
2.7 小结.....	87
第 3 章 提升, 暴力破解和防范	88
3.1 针对应用程序通信认证的暴力破解.....	88
3.1.1 FTP 协议暴力破解原理.....	88
3.1.2 FTP 协议暴力破解实现方法.....	88
实例 3.1 FTP 暴力破解程序代码.....	89
3.1.3 IMAP 协议破解原理.....	92
3.1.4 IMAP 协议破解方法.....	92
实例 3.2 IMAP 协议破解.....	92
3.1.5 POP3 协议暴力破解原理.....	94
3.1.6 POP3 协议暴力破解实现方法.....	95
实例 3.3 POP3 协议暴力破解.....	95
3.1.7 Telnet 协议暴力破解原理.....	98
3.1.8 Telnet 协议暴力破解实现方法.....	98
实例 3.4 Telnet 协议暴力破解.....	98
3.2 防范恶意扫描及代码实现.....	101
3.2.1 防范恶意扫描的原理.....	101
3.2.2 防范恶意扫描的实现方法.....	102

实例 3.5 防范恶意扫描程序的框架.....	102
3.3 小结	106
第 4 章 用代码说话，拒绝服务攻击与防范.....	107
4.1 拒绝服务原理及概述	107
4.1.1 拒绝服务攻击技术类别	107
4.1.2 拒绝服务攻击形式	108
4.2 拒绝服务攻击原理及概述	109
4.2.1 DoS 攻击	109
4.2.2 DDoS 攻击	110
4.2.3 DRDoS 攻击	110
4.2.4 CC 攻击	111
4.3 拒绝服务攻击代码实现	112
4.3.1 DoS 实现代码的原理	112
实例 4.1 典型 UDP Flood 攻击	117
实例 4.2 SYN Flood 攻击代码示例	120
实例 4.3 典型 TCP 多连接攻击程序示例	123
实例 4.4 ICMP Flood 攻击数据包构造	127
实例 4.5 ICMP Flood 攻击	130
4.3.2 DRDoS 攻击的代码实现	132
实例 4.6 InitSynPacket 函数实现过程	134
实例 4.7 InitIcmpPacket 函数实现过程	136
实例 4.8 SYN 反射线程实现方式	136
实例 4.9 ICMP 反射攻击线程实现	138
实例 4.10 开启反射攻击线程	140
实例 4.11 反射攻击线程	140
4.3.3 CC 攻击的代码实现	143
实例 4.12 CC 攻击代码实现	143
4.3.4 修改 TCP 并发连接数限制	146
实例 4.13 修改 TCP 并发连接线程	146
4.4 拒绝服务攻击防范	151
4.4.1 拒绝服务攻击现象及影响	151
4.4.2 DoS 攻击的防范	151
4.4.3 DRDoS 攻击的防范	152
4.4.4 CC 攻击的防范	152
实例 4.14 ASP 程序 Session 认证	153

实例 4.15 ASP 程序判断真实 IP 地址.....	153
4.5 小结	154
第 5 章 你也能开发“病毒”	155
5.1 感染功能描述	155
5.1.1 话说熊猫烧香	155
5.1.2 何为“下载者”	156
5.1.3 感染功能描述	157
5.2 感染型下载者工作流程	165
5.3 感染所有磁盘	166
5.3.1 感染所有磁盘原理	167
5.3.2 感染所有磁盘的实现方法	167
实例 5.1 感染所有磁盘的代码	167
5.4 感染 U 盘、移动硬盘	167
5.4.1 U 盘、移动硬盘感染的原理	167
5.4.2 U 盘、移动硬盘感染的实现方法	168
实例 5.2 U 盘感染实现代码	171
5.5 关闭杀毒软件和文件下载的实现	171
5.5.1 关闭杀毒软件的原理	171
5.5.2 关闭杀毒软件和文件下载的实现方法	172
实例 5.3 关闭杀毒软件和文件下载	172
5.6 结束指定进程	176
5.6.1 结束指定进程的原理	177
5.6.2 结束指定进程的实现方法	177
实例 5.4 结束指定进程	177
5.6.3 暴力结束进程	178
实例 5.5 暴力结束进程	178
实例 5.6 下载执行程序	186
5.7 局域网感染	187
5.7.1 局域网感染原理	187
5.7.2 局域网感染的实现方法	187
实例 5.7 局域网同网段扫描并感染的代码实现	187
实例 5.8 IPC 连接操作	190
5.8 隐藏进程	191
5.8.1 隐藏进程的原理	192

5.8.2	隐藏进程的实现方法	192
5.9	感染可执行文件	193
5.9.1	感染可执行文件的原理	193
5.9.2	感染可执行文件的实现方法	193
	实例 5.9 汇编查找 kernel.dll 的地址	193
	实例 5.10 遍历文件目录查找.exe 文件路径	196
	实例 5.11 全盘搜索.exe 文件	197
5.10	感染网页文件	197
5.10.1	感染网页文件的原理	197
5.10.2	感染网页文件的实现方法	197
	实例 5.12 向指定文件尾部写入代码	197
	实例 5.13 搜索网页文件并调用感染函数	198
	实例 5.14 设置文件隐藏属性	199
5.11	多文件下载	200
5.11.1	多文件下载的原理	200
5.11.2	多文件下载的实现方法	200
5.12	自删除功能	202
5.12.1	自删除功能的原理	202
5.12.2	自删除功能的实现方法	202
	实例 5.15 程序自删除功能	202
5.13	下载者调用外部程序	203
5.13.1	下载者调用外部程序的原理	203
5.13.2	下载者调用外部程序的实现方法	203
	实例 5.16 zxarps.exe 程序帮助信息	203
	实例 5.17 释放资源调用 ARP 攻击程序	206
	实例 5.18 调用 ARP 攻击程序循环攻击 C 段 IP 地址	207
5.14	“机器狗”程序	208
5.14.1	“机器狗”程序原理	208
5.14.2	“机器狗”代码实现	209
	实例 5.19 “机器狗”释放驱动并安装执行的代码实现	209
	实例 5.20 驱动感染 userinit.exe	213
5.15	利用第三方程序漏洞	216
	实例 5.21 迅雷溢出漏洞利用文件 Thunder.js	217
5.16	程序其他需要注意的地方	219
5.16.1	窗口程序的创建	219
	实例 5.22 创建窗口程序的代码实现	219

5.16.2	应用程序互斥处理	220
	实例 5.23 应用程序互斥处理	220
5.16.3	禁止关闭窗口	221
5.17	小结	221

第 6 章 你当然也能开发杀毒程序 222

6.1	下载者的防范措施	222
6.1.1	U 盘感染的防范	222
6.1.2	驱动级病毒的防范	224
6.1.3	阻止第三程序引起的漏洞	226
6.1.4	本地计算机防范 ARP 程序运行	227
6.1.5	其他需要注意的地方	228
6.2	U 盘病毒防火墙的开发	228
6.2.1	U 盘病毒防火墙的功能及实现技术	228
6.2.2	U 盘病毒防火墙的代码实现	229
	实例 6.1 全盘检测 AutoRun.inf 文件	229
	实例 6.2 单个磁盘的扫描检测程序	229
	实例 6.3 删除病毒文件	231
	实例 6.4 格式化磁盘	231
	实例 6.5 调用 System 函数格式化磁盘	232
	实例 6.6 备份文件	232
	实例 6.7 增加注册表启动项	235
	实例 6.8 禁止系统自动播放功能	235
6.3	小结	237

第 7 章 攻防的高难度的动作 238

7.1	Rootkit 与系统内核功能	238
7.1.1	Rootkit 简介	238
7.1.2	Rootkit 相关的系统功能	238
7.1.3	Rootkit 的分类及实现	239
	实例 7.1 IRPS 形式的 Rootkit 编码实现	241
7.2	Rootkit 对抗杀毒软件	243
7.2.1	增加空节来感染 PE 文件	244
	实例 7.2 给程序增加空字节	244
7.2.2	通过 Rootkit 来绕过 KIS 7.0 的网络监控程序	251
	实例 7.3 编程绕过 KIS	252

7.2.3	HIV 绕过卡巴斯基主动防御的方法	253
	实例 7.4 HIV 绕过卡巴斯基	253
7.2.4	关于进程 PEB 结构的修改实现	255
	实例 7.5 进程 PEB 结构的修改实现	255
	实例 7.6 修改 PEB 信息	258
7.2.5	结束 AVP 的批处理	259
	实例 7.7 结束 AVP 的批处理程序	259
7.3	Rootkit 程序实例	262
	实例 7.8 RootKit 程序保护文件功能	262
	实例 7.9 上层应用程序调用 sys 驱动	268
7.4	小结	270
第 8 章	没开发过自己的软件，怎么成大师	271
8.1	远程控制软件简介	271
8.1.1	远程控制软件的形式	271
8.1.2	远程控制软件的特点	272
8.2	远程控制软件的功能	273
8.2.1	反弹连接功能	273
8.2.2	动态更新 IP 功能	273
8.2.3	详细的计算机配置信息的获取	274
8.2.4	进程管理功能	274
8.2.5	服务管理功能	274
8.2.6	文件管理功能	275
8.2.7	远程注册表管理	275
8.2.8	键盘记录	275
8.2.9	被控端的屏幕截取以及控制	276
8.2.10	视频截取	276
8.2.11	语音监听	276
8.2.12	远程卸载	276
8.2.13	分组管理	276
8.3	技术指标	276
8.3.1	隐蔽通信	276
8.3.2	服务器端加壳压缩	277
8.3.3	程序自身保护技术	281
8.3.4	感染系统功能	282
8.4	小结	282

第 9 章 黑客也要懂软件工程 283

9.1 设计远程控制软件连接方式	283
9.1.1 典型的 C/S 型木马连接方式	283
9.1.2 反弹型木马连接	284
9.2 基本传输结构的设计	284
9.2.1 基本信息结构	284
实例 9.1 定义控被控上报基本信息结构	285
9.2.2 临时连接结构	285
实例 9.2 定义临时通信连接结构	285
9.2.3 进程通信结构	285
实例 9.3 定义进程通信结构	286
9.2.4 设计结构成员变量占用空间的大小	286
9.3 命令调度过程的结构设计	287
9.3.1 设计进程传递的结构	287
实例 9.4 定义进程结构变量	287
9.3.2 优化结构成员变量占用空间的大小	287
9.3.3 传输命令结构体定义	288
实例 9.5 构建传输命令结构	288
9.3.4 传输命令结构的设计	288
实例 9.6 定义传输命令结构预定义的宏	288
实例 9.7 进程管理命令的代码实现	290
实例 9.8 双击鼠标事件功能实现	294
实例 9.9 进程信息管理及显示客户端	296
实例 9.10 CProcManageDlg 类中的处理过程	297
实例 9.11 客户端调用 CProcManageDlg 类	297
9.4 小结	298

第 10 章 吃透开发基础功能 299

10.1 反弹端口和 IP 自动更新	299
10.1.1 反弹端口原理	299
10.1.2 更新 IP 模块代码实现	301
实例 10.1 定义 FTP 连接信息	301
实例 10.2 生成 IP 地址更新文件	301
实例 10.3 FTP 连接编程实现	302
10.2 基本信息的获得	303

10.2.1	CGetHDSerial 类获得硬盘序列号	303
实例 10.4	CGetHDSerial 类头文件宏定义	303
实例 10.5	CGetHDSerial 类头文件结构定义	303
实例 10.6	CGetHDSerial 类的方法声明	305
实例 10.7	CGetHDSerial 类的方法实现	306
实例 10.8	GetHDSerial 方法实现	309
实例 10.9	字符转换函数	310
实例 10.10	WinNTReadIDEHDSerial()函数实现	312
实例 10.11	WinNTReadSCSIHDSerial()函数的实现	313
实例 10.12	WinNTGetIDEHDInfo()函数的实现	315
10.2.2	获得服务器端计算机的基本信息	315
实例 10.13	GetClientSystemInfo()获取计算机基本信息	316
10.3	IP 地址转换物理位置	318
10.3.1	QQWry.dat 基本结构	318
10.3.2	了解文件头	319
10.3.3	了解记录区	319
10.3.4	设计的理由	321
10.3.5	IP 地址库操作类	322
实例 10.14	IP 地址库操作类的头文件	322
实例 10.15	IP 地址库操作函数的实现	324
实例 10.16	GetStartIPInfo()函数的实现	325
实例 10.17	GetRecordCount()和 GetStr()的实现	327
实例 10.18	GetCountryLocal()函数的实现	328
实例 10.19	GetStr()和 SaveToFile()函数的实现	329
实例 10.20	IP2Add()函数实现 IP 地址到物理地址的转换	330
实例 10.21	IP 地址检索函数 GetIndex()的实现	330
实例 10.22	GetSIP()和 IP2DWORD()函数的实现	332
实例 10.23	测试函数 Test()的实现	333
10.4	小结	335

第 11 章 让软件成型 336

11.1	进程管理	336
11.1.1	Windows 自带的任务管理器	336
11.1.2	进程管理实现的原理	337
11.1.3	进程管理相关 API 函数介绍	337
11.1.4	代码实现进程管理功能	339

实例 11.1 进程结束编码实现.....	339
实例 11.2 服务器端显示相关信息.....	341
实例 11.3 界面初始化的代码实现.....	342
实例 11.4 初始化进程及客户端枚举进程功能编码实现.....	342
11.2 文件管理	345
11.2.1 服务器端两个重要的函数.....	346
实例 11.5 服务器端两个重要的函数.....	346
11.2.2 客户端对应的两个函数	348
实例 11.6 客户端两个重要的函数.....	348
11.3 服务管理	351
11.3.1 客户端代码	351
实例 11.7 服务管理功能客户端代码实现.....	351
11.3.2 服务器端代码	352
实例 11.8 服务管理功能服务器端实现方式.....	352
11.4 服务器端启动和网络更新	353
11.4.1 服务启动工作函数	354
实例 11.9 服务启动函数的编码实现.....	354
11.4.2 网络下载器的选择和代码实现	354
实例 11.10 HttpDownload 类代码.....	355
实例 11.11 wininet.dll 库编写下载者	379
11.4.3 分析下载文件并且反弹连接	382
实例 11.12 分析下载文件和反弹连接.....	382
11.4.4 上线设置	383
11.5 远程 cmdshell.....	385
11.5.1 客户端代码	385
实例 11.13 远程 cmdshell 客户端代码	385
11.5.2 服务器端代码	386
实例 11.14 远程 cmdshell 服务器端代码	386
11.6 小结.....	387

第 12 章 版本迭代中增加软件功能 388

12.1 屏幕捕捉	388
12.1.1 屏幕捕捉程序结构	388
12.1.2 远程屏幕控制服务器的代码实现	390
实例 12.1 远程屏幕控制.....	390

实例 12.2 屏幕控制客户端编码.....	394
12.2 远程屏幕实现方式.....	397
12.2.1 远程屏幕图像在网络上的传输过程.....	398
12.2.2 屏幕抓取与传输方法及其改进实现.....	398
12.2.3 屏幕图像数据流的压缩与解压缩.....	399
实例 12.3 监控端程序实现方法.....	399
实例 12.4 程序监听连接及显示连接数量的实现方式.....	402
实例 12.5 用户界面初始化及绘制.....	403
实例 12.6 连接显示及界面捕获等功能实现.....	404
实例 12.7 异或法捕获屏幕数据.....	406
实例 12.8 屏幕控制客户端编码实现.....	411
12.3 键盘记录.....	415
12.3.1 客户端执行代码.....	415
实例 12.9 键盘记录客户端编码.....	415
12.3.2 服务器端执行代码.....	420
实例 12.10 键盘记录服务器端功能代码.....	420
12.4 小结.....	421

第 13 章 根据新的需求扩展 422

13.1 客户端历史记录提取与系统日志删除.....	422
实例 13.1 客户端历史记录提取.....	422
实例 13.2 删除日志功能的代码.....	424
13.2 压缩功能的实现.....	424
实例 13.3 zip 压缩功能.....	424
13.3 DDoS 攻击模块.....	425
13.3.1 基本 DDoS 攻击模块.....	425
实例 13.4 DDoS 攻击模块.....	425
13.3.2 UDP 攻击模块.....	428
实例 13.5 UDP 攻击模块.....	428
13.3.3 IGMP 攻击模块.....	430
实例 13.6 IGMP 攻击模块.....	430
13.3.4 ICMP 攻击模块.....	433
实例 13.7 ICMP 攻击模块的实现.....	433
13.3.5 HTTP 攻击函数.....	435
实例 13.8 HTTP 攻击函数的实现方式.....	435