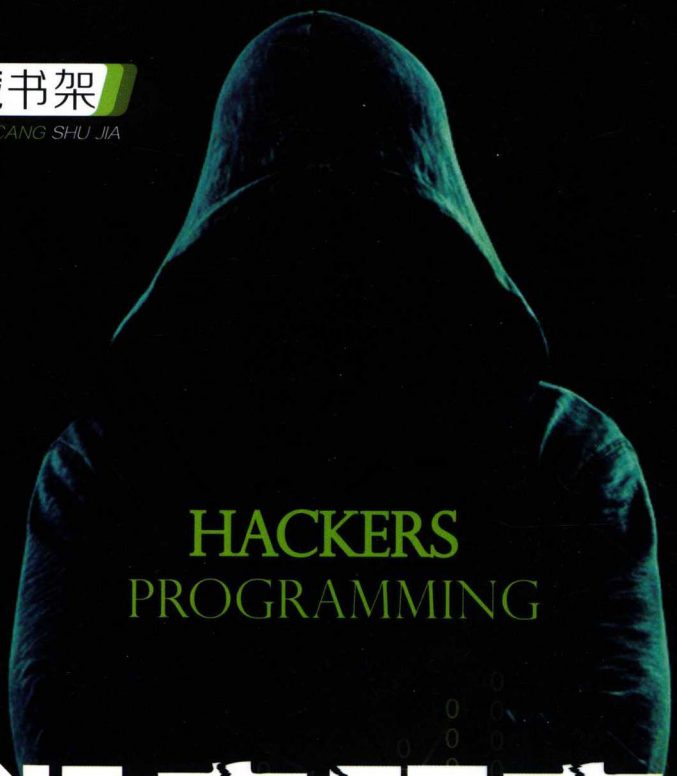
网管员典藏书架

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

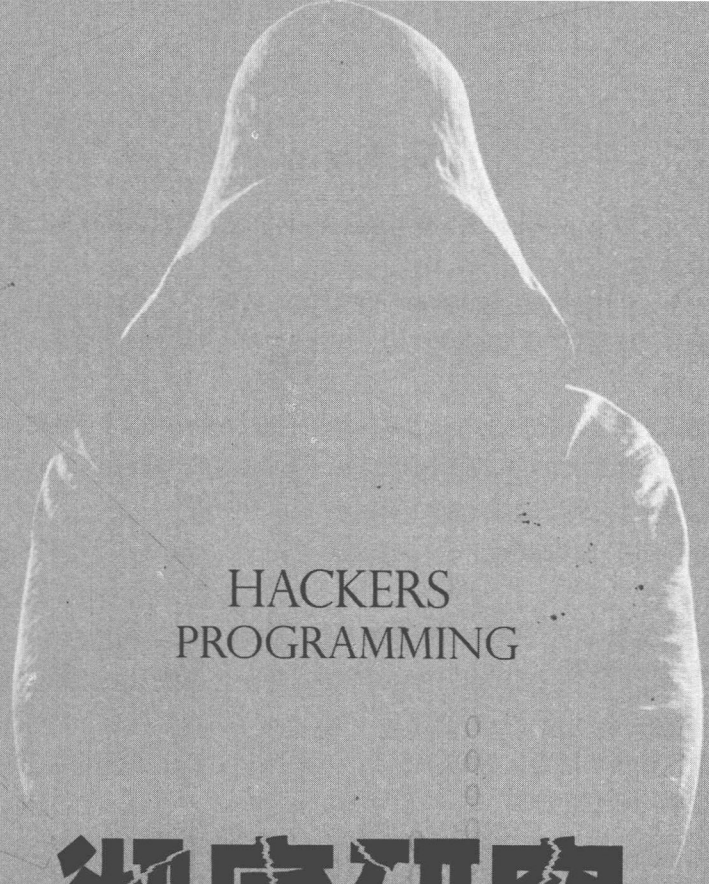
知己知彼，完整再现黑客主流攻击实现方式和攻防案例，提升实战技能

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　　**读者热线电话：**010-63560056
责任印制：赵星辰　　**封面设计：**MXX 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。

“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，以下读者应该仔细研读本书：

- 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

试读结束：需要全本请在线购买： www.ertongbook.com

目　录

试读结束：需要全本请在线购买：www.ertongbook.com

试读结束：需要全本请在线购买：　www.ertongbook.com