Broadview
www.broadview.com.cn

层层剖析由浅入深

形象生动的案例

帮助读者快速掌握使用C/C++和Windows API

进行黑客攻防的技巧和方法

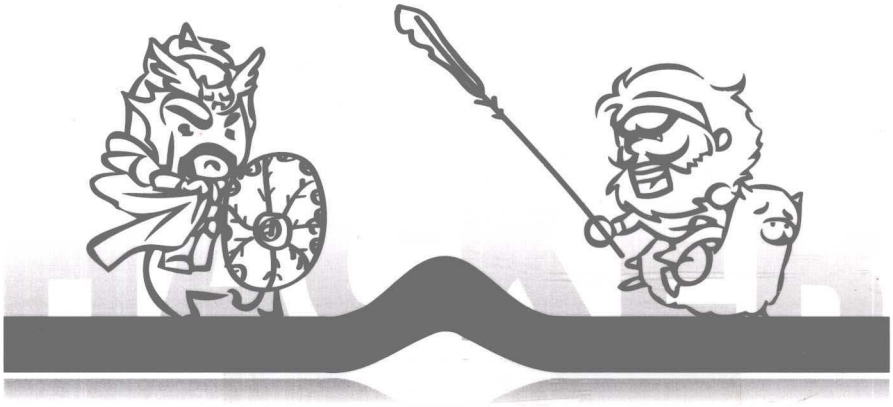
.....

# 小小黑客之路

## ——黑客工具、攻防及防火墙编程入门

葛垚 主编

聂森 苗甦 陈沁茜 陈树林 著



電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

# 小小黑客之路

## ——黑客工具、攻防及防火墙编程入门

聂森 著

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

## 内容简介

信息安全是一面双扇的门，左边写着“黑客”，右边写着“安全”。你推开“黑客”，看见一条路，笑了；他推开“安全”，看见你，也笑了。这就是你的小小黑客之路。

本书正如一幅黑客攻防世界的探险地图，由入门、进阶、高级和综合四个层次组成，以C/C++语言和Windows API为平台，并配合由浅入深、由易到难的各种案例绘制而成。地图中的每一部分都配有生动有趣的情景故事，帮助你理解各种实际发生的现象和应对的方法，帮助你深入探寻各种热门的黑客防守工具的原理及编写技巧，帮助你在轻松幽默的氛围中顺利成长。

本书适合于编程爱好者和信息安全相关专业学生阅读，让我们在学习的道路上结伴同行。



**图书在版编目（CIP）数据**

小小黑客之路：黑客工具、攻防及防火墙编程入门 / 葛垚主编. —北京：电子工业出版社，2011.1
ISBN 978-7-121-11884-5

Ⅰ. ①小… Ⅱ. ①葛… Ⅲ. ①计算机网络—安全技术 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字（2010）第185497号

策划编辑：张月萍
责任编辑：贾　莉
印　　刷：北京市天竺颖华印刷厂
装　　订：三河市鑫金马印装有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路173信箱　　邮编：100036
开　　本：720×1000　1/16　　印张：31　　字数：608千字
印　　次：2011年1月第1次印刷
定　　价：59.00元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至zlts@phei.com.cn，盗版侵权举报请发邮件至dbqq@phei.com.cn。

服务热线：（010）88258888。

# 前言

在网络安全备受重视的今天，黑客及黑客行为也越来越受到人们的关注。很多计算机爱好者都幻想着成为凯文·米特尼克式的世界级黑客人物，但学习资料的匮乏使他们始终怀抱梦想却无法迈入黑客编程的神秘世界。

因此，为了让更多的人领略黑客及黑客编程的魅力，笔者根据自身的学习及经验完成了本书的编写。通过层层剖析书中多个由浅入深、形象生动的案例，读者们可以快速掌握使用C/C++和Windows API进行黑客编程的技巧与方法。

本书共分为入门篇、进阶篇、高级篇和综合篇四部分。在入门篇中，我们首先简要地介绍了黑客、黑客工具及黑客编程中常用的辅助工具，并对一些黑客编程的基础知识，如Windows API的使用、Windows网络编程、用户界面设计等，进行了详细的介绍。进阶篇和高级篇共有七章，分别介绍了七种网络上热门的黑客工具的编写技巧，如端口扫描器、ARP欺骗工具、漏洞利用技术等，案例由浅入深，方便读者学习。在综合篇中，我们又对以上所学的知识进行了综合运用，实现了两个较为复杂的软件：远程控制木马和防火墙。值得一提的是，附录A与附录B中介绍的网络协议和PE格式的基础知识，是黑客编程的基础。

本书使用Visual C++ 2008作为编程平台进行编写和讲解。众所周知，作为微软开发工具，Visual Studio 2008，尤其是其中的Visual C++ 2008的易用性受到程序员们的一致肯定。

本书特色：

（1）本书定位于对信息安全或黑客编程有兴趣的初学者，是一本良好的入门读物。

（2）整本书知识点较为全面，基本包含了黑客编程的各个方面。

（3）书中对相关黑客工具编写的讲解皆通过案例，案例组织由浅入深，形象生动又不乏易用性。

（4）本书使用Visual C++ 2008作为开发平台，方便读者测试和重用代码。

（5）需要原始代码的读者可通过电子邮箱geyao@cqu.edu.cn索取。

我们坚信，持之以恒方能成事。希望在这本书的陪伴下，读者朋友们能坚定地走完黑客编程学习的道路，并能有所感悟，有所收获。

最后，感谢从书的策划到出版一路陪伴着我们的师长、家人和朋友们，你们的默默支持是我们一路走来最大的动力！

由于作者水平有限，疏漏之处在所难免，欢迎读者朋友批评指正。作者服务邮箱为：chenqiok@163.com。

作　者

2010年11月

# 目 录

## 入 门 篇

### 第 1 回 我是黑客，我不是骇客

了解黑客及黑客技术的发展可以拓宽你的视野，使你对黑客有一个更为全面的认识。

# 第 2 回　黑客的编程利器

为你介绍微软强大的开发环境——Visual C++ 2008，它是黑客编程道路上的铺路石，可以使你的编程过程更加灵活、得心应手。



# 第 3 回　黑客眼中的Windows程序设计

为你介绍Windows API、动态链接库、进程、线程以及网络编程等有关黑客编程的基础知识。

## 第 4 回 潜伏在优雅的界面之下

为你介绍界面的绘制和Windows消息机制的基础知识，这是开发高级黑客软件的必备知识。



# 进 阶 篇

## 第 5 回 警报！遭到扫描

一个开放的端口对计算机来说就是一扇打开的门。端口扫描器对目标计算机的各个端口进行扫描，寻找其中对外开放的端口，从而找到网络入侵的突破口。

## 第 6 回 信注册表，没有不可能

病毒、木马往往会借助修改系统注册表的手段来达到突破系统防御的目的。了解注册表编辑器，可以为你编写病毒、木马等黑客工具打下基础。



## 第 7 回 数据窃听风云

数据窃听看上去很酷，动动手，WinPcap嗅探工具就可以为你拦截和分析网络数据。

# 高 级 篇

## 第 8 回 以你的名义欺骗你

冒充他人的骗子不光存在于街头，也存在于计算机之中。编写一个ARP欺骗工具，可以使你实现用别人的“名字”做自己想做的事。

# 第 9 回　病毒，又见病毒

病毒，一个令人深恶痛绝的名字。了解病毒技术及一些简单病毒的编写技巧，可以做到知己知彼、更好地防御它。



# 第 10 回　漏洞是个什么洞

不论是软件上还是硬件上一个小小的缺陷——漏洞，就可以让你的已经防备到牙齿的计算机“溃于蚁穴”。学习如何利用漏洞编写黑客程序是黑客的必修课程。

# 第 11 回 后门是个什么门

作为远程控制木马的基础，后门程序虽然没有强大的控制能力，但其隐蔽性更高。利用Winsock技术就可以轻松实现一个简单的后门程序。



# 综 合 篇

# 第 12 回 特洛伊那匹不吃草的马

木马这个名字跟病毒一样臭名远扬，它可以悄悄地窃取你的账号，监视你在计算机上的一举一动，甚至控制你的摄像头窥探隐私。由于其具有强大的远程控制功能，木马也是黑客最喜爱的工具之一。

## 第 13 回 防火墙说，你不受欢迎

网络防御与网络攻击是永远的盾和矛，了解SPI防火墙如何使用SPI技术对进出本机的数据进行过滤，可以让你在一定程度上了解如何防止黑客的攻击。

# 第 1 回

# 我是黑客，我不是骇客

了解黑客及黑客技术的发展可以拓宽你的视野，使你对黑客有一个更为全面的认识。

自从张飞和曹操相识，他们就结下了梁子，一来蜀营和曹营业务有些对立，二来曹操这厮总喜欢没事就捉弄下张飞，让张飞心中很是不爽。张飞也不是个讲理的主，一看曹操骑到了自家头上，那还得了！不过大家都是“文明人”，曹营也不是他随便能去的，于是张飞满腔怒火，左思来右想去：“这小子，不给他来个下马威，就当我是病猫！不行，一定要好好整整他。不过，不能打架，咱都是文化人啊。那怎么办呢？”翻来覆去一宿，张飞总算想出了一个万全的办法。“嘿嘿，曹操这小子肯定不知道现在流行黑客技术，据说神奇得很，来无影去无踪。而自家蜀营的军师兼好友诸葛亮就精通黑客攻防之道，可以跟他学习一下。”想罢，张飞一阵兴奋，立马从床上蹦起，前往诸葛亮的住处，决心要学习一些黑客攻防的技术，捉弄一下曹操！从此，张飞踏上了黑客攻防的学习之旅……

军师，俺最近饱受曹操欺负，却又无可奈何，特来向您求救啊！

你们两人之间的事情我又如何插手？

曹操那厮太过狡猾，几次与他交手都未能占到便宜，弄得我损兵折将，这可如何是好？

那你要我怎么帮你？

嘿嘿，军师当年在东吴黑战群儒，让俺崇拜得五体投地，不，六体、七体投地，俺想通了，就跟军师学黑客技术，以报一箭之仇，希望军师可以教我两招。

六体投地……那我先问你个问题，什么是黑客？

黑客不就是那种可以在网络世界里飞檐走壁，打家劫舍，进出别人电脑如自家后门的人么。

你这浑人，荒谬，我还是给你说说什么是真正的黑客吧。

## 1.1 什么是黑客

提起黑客，总能让人遐想。媒体的夸张描述、世界著名黑客的传奇人生更是将黑客的神秘推至一个无以复加的地步。正是由于这种片面的了解，主流社会将黑客单纯地定义为了“计算机罪犯”。事实并非如此！黑客，并不是人们眼中的计算机捣乱分子，他们不同于骇客，他们有自己的做事准则和文化。

原来是这样啊，看来我回去要多补补功课才行了。

### 1.1.1 黑客的兴起及发展

黑客（Hacker）一词源于英文动词Hack，意为“劈，砍”，可引申为“干

了一件非常漂亮的工作”。在早期麻省理工学院的校园俚语中，“黑客”一词有“恶作剧”之意，且特指手法巧妙、技术高明的恶作剧。在日本《新黑客词典》中对黑客有这样的定义：喜欢探索软件程序奥秘，并从中增长了其个人才干的人。因此，黑客事实上是一群热衷于追寻新技术的人，而“计算机罪犯”的恶名也只是近几年才产生的。当我们通览黑客的历史能发现：它的产生与发展是建立在时代的背景之上，且与计算机技术的发展紧密相连。因此，“黑客史”其实就是一部计算机发展的历史。

早在20世纪50年代，黑客就出现在了世界著名大学麻省理工学院的实验室中。所谓的“黑客”，是一群精力充沛且热衷于解决难题的年轻人。在60、70年代，“黑客”一词极被推崇，经常被用于指代那些好奇心极强、热衷于各种难题同时又智力超群、对计算机全身心投入的计算机迷。黑客的存在，事实上是对计算机最大潜力的一种探索，为计算机技术的发展做出了巨大贡献。也正是这些黑客，主导了一场个人计算机革命，他们是计算机发展史上的英雄。目前，黑客使用的侵入计算机系统的基本技巧，如破解口令（Password Cracking）、走后门（Backdoor）、安放特洛伊木马（Trojan Horse）等，都是在这一时期发明的。与此同时，黑客的经历也往往能成为一种很好的锻炼，苹果公司创始人之一乔布斯就是一个典型的例子。

在20世纪60年代，计算机还远未普及，因此也没有我们现在所谓的计算机犯罪事件。到了80、90年代，计算机在我们生活中扮演的角色越来越重要，但信息却越来越集中在少数人的手中。黑客们认为，当信息成为一种共享资源时，才是计算机真正融入日常生活的时候。于是他们将注意力转移到如何实现信息共享上。而此时，计算机空间已私有化，成为了一种私有财产，社会也不能再对黑客行为放任不管，必须利用法律等手段来进行控制，黑客活动受到了空前的打击。

我以前还听说过一个词，叫做“骇客”，这个又是怎么回事呢？它和黑客有什么区别呢？

黑客与骇客分属两个不同的族群。对一个黑客来说，成为黑客的过程是学习和提高自身的过程，学会入侵和破解是必要的，但最主要的是编程。毕竟，使用工具是体现别人的思路、依赖别人的表现，而只有自己的程序才是自己最真切的想法。很多安全软件公司的程序员本身就是高明的黑客，因此，黑客技术的发展能带来编程技术的发展和安全技术的进步。

但对于一个骇客来说，他们就没有如此烦琐的学习过程了。他们只追求入侵的快感，不在乎技术的高低精湛，他们不一定会编程，不一定知道入侵的具体细节，仅利用各种现成工具实现入侵的目的。因为骇客的进入门槛低，所以网络上