电脑报 总策划

丛书连续9年再版畅销200万册

电脑硬道理 第9版

黑客攻防

玩家级DIY

电脑报 编

从菜鸟到大虾 练就黑客终极必杀技能

PC DIY

精彩光盘

- 黑客攻防多媒体视频教程
- 常用密码管理工具软件
- 电脑报专用版杀毒软件
- 系统优化、网络安全工具

电脑报电子音像出版社
CEAP ELECTRONIC & AUDIOVISUAL PRESS

电脑硬道理 PC DIY

黑客攻防

电脑报 编

电脑报电子音像出版社
CEAP ELECTRONIC & AUDIOVISUAL PRESS

内容简介

在很多人眼里，“黑客”是一群高深莫测的神秘人物，然而，随着网络的普及和病毒木马的泛滥，更多的人意识到“黑客”其实离我们很近，他就在我们的身边。“黑客”不只是代表破坏、攻击，如今，更多的是代表着网络安全，学习黑客知识，捍卫你的电脑安全，做网络安全卫士，你也行！

电脑硬道理之《黑客攻防》共包括以下四大部分：

基础入门篇：为读者讲解了黑客入门的基础知识，包括黑客应具备的基本技能、黑客必知必会的术语、黑客攻击前的扫描技能以及信息筛选方法；

上手实战篇：这一部分为大家安排了初级黑客攻防实例演练，包括QQ攻击与防范方法、局域网内的安全攻防、常见的密码攻防实例、各类账户欺骗实例剖析；

进阶操练篇：这部分主要讲解更深一层的黑客应用与技巧，包括病毒查杀方法、木马攻防实例、远程控制演练、网吧与网络游戏安全防范、系统与网站漏洞攻防；

安全防范篇：了解黑客攻防的实例操作后，这一部分将为大家介绍黑客防范技巧，包括U盘安全防护、P2P安全防范、使用网络代理隐藏IP、如何进行黑客追踪等内容，让读者知己知彼，做一名安全高手。

警告：文中涉及到的黑客攻防相关内容，仅供读者学习之用，如用于非法用途，后果自负！

光盘要目

1.电脑报专用版安全工具（2款）
（《木马清除大师》、《FileGee个人同步备份系统》）
2.系统与网络安全辅助工具（5款）
3.密码管理工具（5款）
4.Windows优化工具（4款）
5.黑客攻防视频教程（12部）

书　　名：黑客攻防
编　　者：电脑报
技术编辑：李　勇
封面设计：陈鲁豫
出版单位：电脑报电子音像出版社
地　　址：重庆市双钢路3号科协大厦
邮政编码：400013
对外合作：(023)63658933

发　　行：电脑报经营有限责任公司
经　　销：各地新华书店、报刊亭
CD生产：四川省蓥山数码科技有限公司
文本印刷：重庆市联谊印务有限公司
开本规格：787mm×1092mm 1/16　23印张　400千字
版　　号：ISBN 978-7-900729-72-9
版　　次：2008年5月第1版　2008年5月第1次印刷
定　　价：32.00元(1CD+配套书)

挑战自我，享受DIY的乐趣

在这愈发崇尚自我的时代，
DIY 已不局限于Do it yourself（自己动手）的范畴。
DIY不知不觉进入到2.0时代，它其实代表着一种精神，一种自由。
而创意、时尚、个性、体验、享受、互动，俨然一张张鲜明的DIY 2.0新时代标签。

1996 年，DIY 的理念由《电脑报》在国内率先提出，并随即在电脑爱好者中迅速流传开来，深受电脑商家和用户的推崇，以致一批又一批电脑玩家乐此不疲。DIY 甚至一度成为性价比极高的组装电脑的代名词。

透过电脑应用的发展历程不难看出，正是 DIY 精神的深入人心，推动了国内个人电脑应用的迅速普及。而今，随着信息技术的不断升级，信息化应用得以广泛而深入地推进，DIY 也不断被赋予新的内涵，不知不觉已悄然进入到了彰显个性的 DIY 2.0 时代，DIY 的精神进而得以发扬光大：除传统硬件的选购、组装、改造、升级 DIY 以外，软件 / 系统的潜能挖掘、网络应用的按需定制、故障怪象的诊断排除、网络黑客的有效防御、酷炫作品的完美打造……也统统被纳入了 DIY 的领地。新一代 DIY 迷们通过自己动手、自学、自助，实现一项项目标应用或任务，努力挑战想象力的极限，充分享受着 DIY 带来的乐趣与成就。

如果说DIY 1.0的核心在于“创造性价比”，那么DIY 2.0的核心就是“以人为本”。在 DIY 2.0 精神的召唤下，不仅电脑应用手段大为丰富，更多产品和服务的需求也被激发了出来。在 DIY 2.0 时代，可以说只有你想不到的，没有做不到的。

1999 年，电脑报组织资深 DIY 玩家和电脑高手精心编写《电脑硬道理》丛书并适时推出，实际上将当时电脑 DIY 的经验和精髓结集成册，系统展现给了广大读者。丛书自出版以来，已连续 9 次再版，累计发行量超过 200 万册。《电脑硬道理》丛书，事实上成为电脑用户及时了解最新电脑应用的风向标，也是广大电脑爱好者首选的经典电脑实战手册。

由于电脑技术更新换代快，电脑应用也不断翻新，我们广泛听取了众多电脑专家和读者的意见，并顺应目前电脑 DIY 的趋势和潮流，选取最受广大用户关注的电脑装机、系统操作、故障排查、硬件维修、网管实战、黑客防范等主要应用，重新策划和编写了这套新版的《电脑硬道理 2008》丛书。《电脑硬道理 2008》丛书延续了历年《电脑硬道理》的风格，始终将通俗、实用放在首位，并结合 DIY 2.0 的最新潮流，为广大读者提供最新鲜、最全面、最权威的电脑应用资讯和实战技巧，是广大电脑爱好者提升应用水平不容错过的一道饕餮大餐！

电脑报

2008 年 5 月

阅读与进阶快速通道

	入口	目的
基础入门	§1 黑客入门第一课	常用的黑客手段 黑客必知必会的术语 查看隐藏进程和远程进程
	§2 黑客攻击前的准备工作	网站信息探测 信息的筛选 扫描与嗅探实例分析
上手实战	§3 QQ攻击与防范实例	QQ强制视频聊天 “假”密码保护陷阱 QQ聊天记录泄秘 QQ密码本地监听
	§4 局域网攻防实例	Windows XP安全共享 修改组策略增强共享安全 Windows Vista系统安全共享
	§5 密码攻防实例	Syskey双重加密与解除 文件和文件夹密码攻防 办公、压缩文档密码攻防
	§6 账户欺骗实例剖析	管理员账户删除与伪造 识破管理员组的Guest账户 防范假终端管理员 防范邮箱账户欺骗
进阶操练	§7 病毒查杀与防范实例	防范邮件附件病毒 全面防范网络蠕虫 搭建虚拟机深入理解病毒发作
	§8 木马攻击与防范实例	木马的攻击过程分析 如何检测木马的存在 防范变幻网页木马 专业工具杀木马
	§9 远程控制攻防实例	Windows XP自带远程控制工具 Windows Vista远程桌面连接 远程管理主机的利用
	§10 网游与网吧攻防实例	网络游戏“盗号”揭秘 解读网站充值欺骗术 防范服务器遭遇DoS攻击 网游外挂完全解密
	§11 系统与网站漏洞攻防实例	系统漏洞检测与修复 扫描局域网内计算机的安全漏洞 网站提权漏洞攻防 网站数据库攻防
安全防范	§12 网络代理与黑客追踪	用“代理猎手”找代理 组合代理服务器的深入应用 实战IP追踪术
	§13 网络安全与黑客防范	用安全卫士清理恶意软件 P2P网络安全防护 多功能的黑客工具箱 数字签名揪出可疑文件 影子系统保障系统安全

CONTENTS 目录

基础入门篇

第一章 黑客入门第一课

第二章 黑客攻击前的准备工作

目录 CONTENTS

上手实战篇

第三章 QQ攻击与防范实例

CONTENTS 目录

第四章 局域网攻防实例

第五章 密码攻防实例

目录 CONTENTS

第六章 账户欺骗实例剖析

CONTENTS 目录

进阶操练篇

第七章 病毒查杀与防范实例

目录 CONTENTS

第八章 木马攻击与防范实例

第九章 远程控制攻防实例

CONTENTS 目录

第十章 网游与网吧攻防实例

目录 CONTENTS

第十一章 系统与网站漏洞攻防实例

CONTENTS 目录

安全防范篇

第十二章 网络代理与黑客追踪

第十三章 网络安全与黑客防范

目录 CONTENTS

01

基础入门篇

第一章
黑客入门第一课

在许多人眼里，“黑客”（Hacker）是一群高深莫测的神秘人物，他们利用掌握的技术肆意展开各种攻击，他们无往而不利……再加上一些媒体对黑客事件不负责任地夸大报道，使得黑客以及黑客技术对普通的电脑用户而言，无形中就多了几许神秘的色彩！其实，黑客以及黑客技术并不神秘，也并不高深。本章就带领大家认识黑客，学习黑客的入门知识。

1.1 黑客要具备哪些技能

怎样才能做一名黑客呢？黑客都常用哪些“绝招”来进行攻防呢？很多人由于对电脑安全防御和黑客入侵原理缺乏必要的了解，常常被黑客攻击了都还蒙在鼓里。因此，本节将一些常见的黑客攻击手段进行简单的介绍。

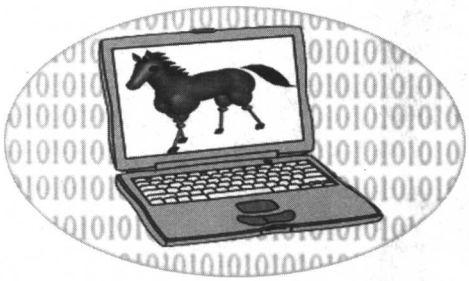
1.1.1 常用的黑客手段

在网络不断走向高速化的今天，全球网民的总量天天都在增加，再加上电脑安全配置不尽相同、用户安全意识有高有低，这都给黑客提供了“练兵场”。因而，黑客可以实施的手段各种各样。

1.木马与病毒

木马全称为“特洛伊木马”，其名源于古希腊神话。传说古希腊人围困特洛伊城，久攻不下。后来想出了一个妙计，让一些死士躲进巨大的木马中。大部队假装撤退而将木马摈弃于特洛伊城下，让敌人将其作为战利品拖入城内。夜晚特洛伊人正在觥筹交错、庆祝胜利的时候，木马内的士兵乘机爬出来，与城外的部队里应外合而攻下了特洛伊城。

在计算机安全领域中，之所以将一种由服务器端和客户端两部分组成的程序叫做“特洛伊木马”，是因为其服务器端在通过种种欺骗（伪装）的方法进入被入侵主机后，可以悄悄地打开系统的一扇门（端口），这样其客户端就可以立即与其相连接，从而一举攻下系统的完整控制权。



木马示意图

木马一般有两种功能，一种是利用此类程序潜入用户电脑，窃取所需要的数据；二是利用在目标电脑中植入服务器端后，黑客在自己的电脑中通过客户端进行鼠标、文件管理等操作。