学电脑从入门到精通

精品图书 + 多媒体演示 + 超值赠品 = 您的最佳选择！
入门→提高→精通→实战，助您从新手变成高手！

黑客攻防从入门到精通

九州书源
刘凡馨 常开忠 等编著

赠超值DVD

专为本书开发的15小时多媒体教学

盘中免费赠送超值大礼包：

- 电脑技巧12000例查询软件
- 15小时《新手学电脑》多媒体教学演示
- 15小时《Word/Excel应用》多媒体教学演示
- 15小时《Windows Vista操作系统》多媒体教学演示
- 15小时《电脑选购/组装/维护/故障排除》多媒体教学演示

清华大学出版社

学电脑从入门到精通

黑客攻防从入门到精通

九州书源

刘凡馨　常开忠　等编著

清华大学出版社

北　京

内 容 简 介

本书是一本关于黑客攻防的书籍，主要内容包括黑客的基础知识、黑客工具的使用、黑客攻击前的准备工作、漏洞攻防、密码攻防、即时通讯工具 QQ 和 MSN 攻防、电子邮件攻防、ARP 欺骗攻防、木马攻防、远程监控攻防、后门攻击与痕迹清除、网络安全防御、提升电脑网络防御性能和建立安全防御体系等知识。

本书内容丰富、实用，共分为 3 篇 14 章，根据学习的难易程度以及在实际工作中应用的轻重顺序安排知识点，每章后面均附有“知识问答”和“知识关联”，在每页的下方还提供了与本页知识相关的操作技巧、注意事项或作者经验谈，以尽可能多地为读者设想，解决读者学习中的疑问。

本书适合电脑维护人员、IT 从业人员和对黑客攻防和安全维护感兴趣的用户自学参考，也可作为大中专院校和各种电脑培训班的教材。

图书在版编目（CIP）数据

黑客攻防从入门到精通/刘凡馨，常开忠等编著. —北京：清华大学出版社，2010.11
（学电脑从入门到精通）

ISBN 978-7-302-21667-4

I. ①黑… II. ①刘… ②常… 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 114252 号

责任编辑：朱英彪
版式设计：侯哲芬
责任校对：姜　彦
责任印制：何　芊
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：北京市世界知识印刷厂
装 订 者：三河市金元印装有限公司
经　　销：全国新华书店
开　　本：190×260　**印　张**：22.5　**插　页**：1　**字　数**：548 千字
（附 DVD 光盘 1 张）
版　　次：2010 年 11 月第 1 版　　**印　　次**：2010 年 11 月第1 次印刷
印　　数：1～7000
定　　价：43.00 元

产品编号：036749-01

前　言

先讲讲这套书的故事吧！

“学电脑从入门到精通”系列图书的第 1 版自 2008 年出版以来，以其科学的知识分布、翔实丰富的图书内容、清新的阅读环境，受到广大读者的热烈欢迎，曾在全国各大书店畅销一时，不同层次、不同年龄段的读者通过这套书学习并掌握了电脑相关技能，给工作与生活带来了希望与乐趣。

在读者来信中，有的读者反映一些知识落后了，希望我们能推出新的版本；有的读者希望能增加网上开店、黑客攻防等新的内容。为了满足广大读者的需求，我们对“学电脑从入门到精通”系列图书进行了全新改版和内容更新，并增加了新的、流行的图书品种，内容更加贴近读者。因此不管您处于哪个层次、哪个年龄段，只要您还不会用电脑，而且希望学到的东西不仅仅是“皮毛”，那么本套书一定可以帮您实现这个愿望。

这本书为谁而写？

《黑客攻防从入门到精通》一书针对各个层次和年龄段的人群。对于掌握了一定电脑技术，想进一步学习黑客技术的电脑用户，本书将为您介绍成为一个黑客的基本条件和一些基础知识；对于对黑客技术非常感兴趣的电脑爱好者及学生，本书将为您讲解黑客攻击的基本方法和基本防御措施；对于迫切需要综合提高黑客攻防技能的初学者，本书将为您介绍如何利用专业软件和操作系统设置来防御黑客攻击的方法。

本书的特点有哪些？

本书经过我们精心策划和编写，主要有以下一些特色。

◆ **科学的知识分布**

本书内容按照入门篇、提高篇和精通篇进行划分，将知识点根据读者学习的难易程度，以及在实际工作中应用的轻重顺序来安排，真正为读者的学习考虑，也让不同读者能在学习过程中有针对性地选择学习内容。如果我们把学电脑的整个过程比作三级阶梯，那么每一篇就是一级阶梯，学习完一篇就能达到该阶梯所对应的高度。

◆ **清新的阅读环境**

本书立足于实用性，并不像传统的教科书那样语言枯燥无味，理论知识和实例效果生硬、无实际使用价值，而是深入考虑读者的实际需求，将内容版式设计得清新、典雅，内容实用，就像一位贴心的朋友、老师，在您面前将枯燥的电脑知识娓娓道来。

◆ **专业的知识体现**

为了体现本书的专业性和实用性，书中特别在每页的底部以灰色底纹隔开一段区域，

在“入门篇”、“提高篇”、“精通篇”中分别设置“行家提醒”、“专家指导”、“精讲笔录”等板块，对正文知识进行补充与提升。

◆ **光盘视频教学**

本书配有多媒体教学光盘，收集了书中的所有实例素材和效果文件，并采用互动式多媒体教学，针对学习进度精心录制了大量的视频讲解，覆盖全书所有知识点，使读者快速学会相关操作。

本书讲些什么？

本书分为 3 篇、共 14 章，主要内容介绍如下。

◆ **入门篇（1~3 章，黑客的基础知识）**：主要讲解了黑客的基本情况、黑客必须掌握的工具和命令、成为黑客的理论条件、各种黑客常用的攻击工具、组建测试系统、文件隐藏和传输技术、攻击隐藏技术和收集网站信息等知识。

◆ **提高篇（4~10 章，黑客常用的攻击手段和防御方法）**：主要讲解了漏洞的基础知识、利用漏洞攻击、修补漏洞、破解各种密码、保护电脑中的密码、攻击 QQ 漏洞、攻击 QQ 密码、保护 QQ、MSN 安全攻防、电子邮件攻防、邮箱炸弹、压缩文件攻防、网络欺骗技术、ARP 欺骗攻击的演示和防御、认识木马、第二代和第三代木马攻防、使用木马清除软件和远程监控攻防等知识。

◆ **精通篇（11~14 章，如何设置电脑来防御黑客攻击）**：主要讲解了后门攻击、痕迹清除、阻止间谍软件、阻止恶意网络广告、阻止流氓软件入侵、常见的网络安全防护工具、设置 Windows 操作系统、设置系统组策略、设置注册表、备份与恢复数据、使用 360 杀毒和 360 安全卫士等知识。

本书的创作团队

我们创作本书的宗旨是保证所有知识点都能让读者学有所用，鉴于这个宗旨，参与本书编写的人员在电脑书籍的编写方面都有较高的造诣，他们是刘凡馨、常开忠、任亚炫、丛威、范晶晶、唐青、陈晓颖、陆小平、简超、羊清忠、李显进、赵云、杨颖、张永雄、李伟、余洪、袁松涛、杨明宇、牟俊、宋玉霞、宋晓均、向利、徐云江、张笑、赵华君、骆源、陈良、彭启良、刘成林、林涛、程云飞、汪科、方坤、蒲涛、张春梅、官小波、吴永恒和董娟娟。在创作本书的过程中，他们花费了大量心血，在此表示感谢。虽然对于本书我们已尽可能做到更好，但可能其中仍有疏漏和不足之处，欢迎读者朋友不吝赐教。

怎么解决学习的疑惑？

如果您在学习的过程中遇到什么困难或疑惑，可以联系我们，我们会尽快为您解答。我们的联系方式是 QQ 群众：122144955，E-mail：book@jzbooks.com，网址：http://www.jzbooks.com。

目 录

入门篇

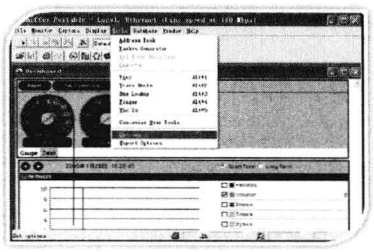
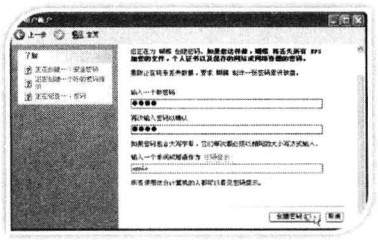
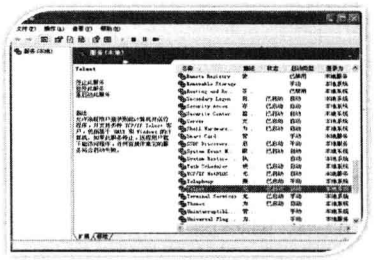
提高篇

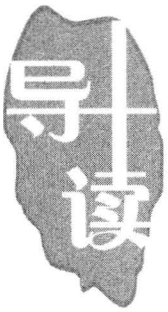
精通篇

入门篇

第 1 章

初识黑客攻击



什么是黑客？黑客攻击的目的是什么？具备怎样的条件才能成为黑客？黑客需要学习哪些技能和知识？相信每个想了解黑客和想成为黑客的人最初都会有以上疑问。本章将针对上述问题，联系相关的知识，对黑客的历史和现状、黑客的各种行为准则、黑客必须掌握的各种技能和工具进行详细的介绍，帮助大家了解黑客，熟悉黑客常用的命令和工具，为电脑的安全防御提供保障。

- 认识神秘的黑客
- 进一步了解黑客
- 成为黑客的条件

1.1 认识神秘的黑客

什么是黑客？黑客的过去和现在是怎样的？未来的黑客又会发展成怎样？下面分别进行讲解。

1.1.1 什么是黑客

黑客最早源自英文 hacker，本意是指热心于计算机技术、水平高超的电脑专家，尤其是程序设计人员，因此，“黑客”一词早期在美国的电脑界是带有褒义的。黑客不干涉政治，不受政治利用，他们的出现推动了电脑和网络的发展与完善。黑客所做的不是恶意的破坏，他们是一群纵横于网络上的“大侠”，追求共享、免费，提倡自由、平等。黑客的存在是由于电脑技术的不健全，从某种意义上讲，电脑的安全需要更多黑客去维护。

但到了今天，因为系统、网络和软件不可避免地会存在安全漏洞，而黑客的出现就是为了找出并弥补这些漏洞，但有些黑客在找出安全漏洞之后，为了显示自己的本领和成就，会对别人的电脑大肆进行恶意破坏。所以，现在各种媒体中的“黑客”一词已经被用于泛指那些专门利用电脑网络搞破坏或恶作剧的家伙，对这些人的正确英文叫法是 Cracker，也可翻译成“骇客”。也正是由于这些人的出现玷污了“黑客”一词，使人们把黑客和骇客混为一体，黑客也被人们认为是在网络上进行破坏的人。因此，“黑客”一词一般有以下几种涵义：

- 对（某领域内的）编程语言有足够了解，可以不经长时间思考就能创造出有价值的软件的人。
- 恶意（一般是非法的）破解或破坏某个程序、系统及网络安全的人。这类人常对那些符合第一种意义的黑客造成严重困扰，通常媒体将这群人称为“骇客”（Cracker），有时这群人也被称为“黑帽黑客”。
- 通过破解某系统或网络以提醒该系统所有者系统存在安全漏洞的人。这群人往往被称为“白帽黑客”、“匿名客”（Sneaker）或“红客”。这样的人大多是电脑安全公司的雇员，他们在完全合法的情况下攻击某系统。
- 通过知识或猜测而对某段程序做出（好的）修改，并改变（或增强）该程序用途的人。

1.1.2 黑客的发展

黑客存在于全世界范围内，从最初美国产生的第一批黑客，直至如今的国内外，都存在众多的黑客。

1. 国际黑客的发展史

国际上对黑客的发展主要可划分为以下几个阶段。

行家提醒

“脚本小子”指那些完全没有或仅有一点点骇客技巧，只是按照指示运行某种骇客程序来达到破坏目的的人。

- **20 世纪 50 年代**：一般认为，黑客起源于 20 世纪 50 年代麻省理工学院的实验室中，他们精力充沛，热衷于解决难题。
- **20 世纪 60 年代**：进入 20 世纪 60 年代后，黑客代指独立思考、奉公守法的计算机迷，他们利用分时技术允许多个用户同时执行多道程序，扩大了计算机及网络的使用范围。
- **20 世纪 70 年代**：20 世纪 70 年代后，黑客倡导了一场个人电脑革命，他们发明并生产了个人电脑，打破了以往电脑技术只掌握在少数人手里的局面，并提出了电脑为人民所用的观点，这一时代的黑客是电脑史上的英雄，在这一时期，黑客们也发明了一些侵入计算机系统的基本口令和技巧，如破解口令（Passwordcracking）、开天窗（TraPdoor）、进入后门（Backdoor）和安装木马程序（Trojan Horse）等。
- **20 世纪 80 年代**：进入 20 世纪 80 年代，黑客的代表是电脑软件工程师，这一代黑客为个人电脑设计出了各种应用软件。而就在此时，随着电脑重要性的提高，各种大型数据库也逐步建立起来，但这些信息不能被公开使用。于是，黑客开始为信息的共享而奋斗，这时黑客开始频繁入侵各大电脑网络。
- 20 世纪 90 年代至今：如今的黑客队伍人员杂乱，既有善意的以发现计算机系统漏洞为乐趣的“电脑黑客”（Hacker），又有玩世不恭、爱好恶作剧的“电脑黑客”（Cyberbunk），还有纯粹以私利为目的，任意篡改数据，非法获取信息的“电脑黑客”（Cracker）。

2. 国内黑客的发展史

在中国 Internet 技术的成长道路上，中国黑客与安全事业的发展历程也是交织在一起的，国内黑客的发展主要可分为以下 3 个阶段。

- **中国黑客的起源**（1994—1996 年）：这个时期是中国 Internet 刚刚开始发展的萌芽时期，各地电脑发烧友最大的乐趣就是复制一些小游戏和 DOS 等软件类产品，于是诞生了最早的黑客，或者说是“窃客”。
- **中国黑客的成长**（1997—1999 年）：这一时期，中国各个大中城市的 Internet 信息港已经初具规模，在这一环境条件下，产生了众多的黑客。他们所掌握的技术主要是邮箱炸弹，后来诞生了特洛伊木马，也就是网络间谍 NetSpy，随后少量的国产工具开始小范围流行于中国黑客之间。
- **中国黑客的发展**（2000 年至今）：2000 年后，中国的黑客队伍迅速扩大，众多的黑客工具与软件使得进入黑客的门槛大大降低，黑客不再是网络高手的代名词。黑客思想开始逐渐成熟，黑客道德与黑客文化的讨论和延伸也让中国黑客逐步重返自然状态，致力于对网络安全技术的研究。

1.1.3 黑客的现状和未来

相对于现在的中国黑客现状来说，中国黑客针对商业犯罪的行为并不多，报刊出现的一些所谓的商业黑客犯罪行为，实际上多采用物理手段，而非网络手段。从根本上说，中国黑客的现状和未来都是令人担忧的。

操作提示

中国黑客联盟自 1999 年创建至今，已经历了十几年。这些年的发展，为中国网络留下了不可磨灭的印象，也因此成就了众多的网络安全专家。

1. 现状

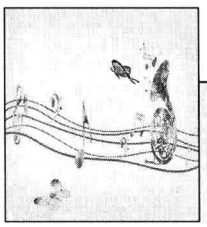
中国黑客的现状主要表现在以下几个方面。

- **数量庞大但良莠不齐**：目前，国内的黑客组织良莠不齐，很多人以一些简单程序迷惑不知情的网民，甚至打着黑客的旗号招摇撞骗。
- **缺乏明确的战略目标与高度的社会责任感**：不少黑客尚处于炫耀个人实力的阶段，没有意识到自己身上肩负的社会责任与时代使命，缺乏危机意识，甚至为违法犯罪分子所利用。
- **一些违法犯罪行为日益猖獗**：目前大部分网民上网时都遇到过病毒和木马的攻击，很多网民甚至遇到过账号或密码被盗的问题。网络安全隐患使网民对 Internet 的信任度大大下降，从而制约了电子商务、网络支付等交易类市场的发展。
- **部分积极作用**：客观地说，黑客行动对网络安全起到了启发作用，没有黑客，就没有网络安全这个概念。同时，一批黑客高手已转变为网络安全专家，研发出众多安全技术和安全软件，对我国计算机和网络的发展做出了贡献。

2. 未来

针对黑客的现状，在未来黑客的发展上有以下 3 方面的内容值得参考。

- **明确战略目标**：黑客应首先明确战略目标以及黑客存在的价值观念，把维护国家和人民利益作为最高准则，建立起维护我国网络安全的阵线，大量培养我国的信息后备人才，激发人民的参与热情。
- **建立与完善组织**：对于黑客组织来说，应结合活动规则，建立一套现代条件下的“黑客制度”。
- **与违法犯罪行为的关系**：黑客组织需要与犯罪行为明确划清界限，要严厉打击黑客群体中的犯罪行为。



1.2 进一步了解黑客

黑客为什么要进行攻击？黑客有什么行为准则？要成为黑客有哪些必须要掌握的命令和工具？下面就针对这些问题分别进行讲解。

1.2.1 黑客攻击的目的

因为黑客具有随意入侵别人的电脑，查看其中信息，然后在被攻击者毫不知情的情况下悄然退出的能力，使得很多人对他们有极强的崇拜心理，并产生了极高的学习黑客技术的欲望，并在了解了黑客攻击技术之后不计后果地进行尝试，给网络造成极大的安全威胁。

从基本的入侵到来去自如，从浏览别人电脑内的文件到破解机密信息，从传播病毒木马到造成别人电脑系统崩溃和硬盘分区表损坏等，从恶意篡改网页到攻击服务器使其瘫痪，这都是黑客们相互炫耀的资本。对于一些刚学会黑客技术、行为偏激的人来说，更是如此。

行家提醒

无论电脑的防范有多严密，安全指数有多高，只要它的系统是由人类所设计的，那么必然会存在缺陷。黑客对电脑信息进行搜集的目的就是为了找出这些缺陷并加以利用。

黑客攻击的目的主要有以下几种。

1. 进程的执行

如果黑客在连接到目标主机后，只是运行了一些简单的、仅消耗电脑系统的CPU资源的程序，那么，这并不是真正的目的。因为有些程序只能在一种系统中运行，到了另一种系统中将无法运行，一个特殊的例子就是一些扫描只能在UNIX系统中运行，在这种情况下，攻击者为了攻击的需要，往往就会找一个中间站点来运行所需要的程序，并且可以避免暴露自己的真实目的，即使被发现了，也只能找到中间的站点地址。

另外一种情况是，如果网络中有一个站点能够访问另一个严格受控的站点或网络，黑客为了攻击这个站点或网络，可能会首先攻击这个中间的站点。这种情况对被攻击的站点或网络本身可能不会造成破坏，但有很多潜在的危险。首先，它占用了大量的系统处理时间，尤其在运行一个网络监听软件时，使得一个主机的响应速度变得非常缓慢。另外，将严重影响目标主机的信任度，因为黑客借助的目标主机对目标主机造成损失时，会将责任转嫁到管理员身上，这样可能导致目标主机损失一些受信任的站点或网络。还有一种可能是黑客将账单转嫁到目标主机上，在网上获取收费信息。

2. 获取文件和传输中的数据

黑客攻击的最大目标就是系统中的重要数据，因此黑客登录目标主机，或使用网络监听进行攻击时，一般都会复制当前用户目录下的文件系统中的用户名或密码。

3. 获取超级用户的权限

对于操作系统来说，超级用户的权限意味着可以做任何事情，这对黑客无疑是一个莫大的诱惑。在UNIX系统中，支持网络监听程序必须拥有这种权限，因此在一个局域网中，只有掌握了一台主机的超级用户权限，才能掌握整个子网。

4. 对系统的非法访问

有许多操作系统或网络是不允许其他用户访问的，如一个公司或组织的网络。因此，黑客通常对这种系统进行攻击，这种攻击的目的并不一定要做什么，只是以一种非正常的行为来得到访问的权限。

5. 进行不许可的操作

只要是用户，都会被允许访问某些资源，但通常受到许多的限制。在UNIX系统中，如果没有超级用户的权限，将无法做许多事情，于是很多只有普通权限的黑客，总想得到一个更大的权限。在Windows操作系统中也一样，许多黑客都有意无意地去尝试尽量获取超出允许的一些权限，于是便寻找管理员在设置中的漏洞，或者找一些工具突破系统的安全防线，如特洛伊木马就是一种使用较多的手段。

6. 拒绝服务

拒绝服务是一种有目的的破坏行为，其攻击方式包括将连接局域网的电缆接地；向域名服务器发送大量的无意义的请求，使其无法完成从其他主机传输的名字解析请求；在网络中制造大量的封包，占据网络的带宽并延缓网络的传输等。

操作提示

除了用物理的方法破坏别人的电脑和重新安装操作系统外，对电脑的其他破坏黑客基本上都能做到。