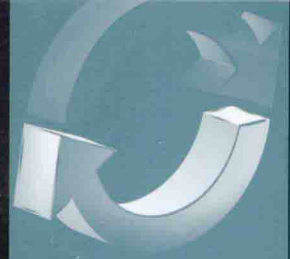
学电脑从入门到精通



THE SECRETS OF BEING AN EXPERT
IN COMPUTER FROM A BEGINNER

黑客攻防
从入门到精通
（实战版）

王叶 李瑞华 等编著

- 简单易学：从易到难、循序渐进，图文并茂、通俗易懂
- 实用性强：网络真实攻防技术、案例+技术的讲解模式
- 技巧与窍门：丰富的攻防技巧与窍门、帮读者答疑解惑，掌握攻防技术

机械工业出版社
China Machine Press

黑客攻防
从入门到精通
（实战版）

王叶 李瑞华 等编著

图书在版编目（CIP）数据

黑客攻防从入门到精通（实战版）/ 王叶等编著 . —北京：机械工业出版社，2014.6

ISBN 978-7-111-46873-8

I. 黑… II. 王… III. 计算机网络－安全技术 IV. TP393.08

中国版本图书馆 CIP 数据核字（2014）第 117444 号

本书紧紧围绕黑客攻防技术，主要介绍从零开始认识黑客，信息的扫描与嗅探，系统漏洞、病毒、木马的入侵与防范，远程控制技术，加密与解密技术，网络欺骗与安全防范，QQ 账号攻防策略，系统和数据的备份与恢复，间谍软件的清除和系统清理以及常见的网络安全防护工具等内容。本书力求以简单明了的语言向读者清晰讲解并使用户对黑客攻防技术形成系统的了解，从而更好地防范黑客的攻击。

本书的内容从易到难、循序渐进、图文并茂、通俗易懂，适于广大网络爱好者以及计算机维护人员阅读。

黑客攻防从入门到精通（实战版）

王叶　等编著

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码：100037）

责任编辑：李华君　　责任校对：殷　虹

印　　刷：北京瑞德印刷有限公司　　版　　次：2014 年 7 月第 1 版第 1 次印刷

开　　本：185mm × 260mm　1/16　　印　　张：22.5

书　　号：ISBN 978-7-111-46873-8　　定　　价：59.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

客服热线：（010）88378991　88361066　　投稿热线：（010）88379604

购书热线：（010）68326294　88379649　68995259　　读者信箱：hzjsj@hzbook.com

前言

如今，网上消费、投资、娱乐等已占据了人们生活的一大部分，那么，如何保证网络账户、密码安全已成为广大用户非常关注的问题，尤其是经常听闻身边好友QQ被盗、账号丢失等，防御黑客入侵已经成为一个不得不重视的问题，因而，作者编写了此书。

本书共分为14章，主要内容如下。

第1章：介绍学习黑客攻防前首先要了解的基础知识，包括IP地址、端口、黑客常见术语及命令，以及黑客在攻击前做的准备工作——创建虚拟测试环境。

第2章：介绍黑客攻击前对信息的扫描与嗅探以及网络监控技巧。

第3章：介绍系统常见漏洞入侵与防范技巧。

第4章：认识病毒并介绍病毒入侵与防御技巧以及制作简单的病毒。

第5章：认识木马并介绍了木马的伪装与生成、加壳与脱壳以及木马的清除。

第6章：介绍通过入侵检测技术自动检测可疑行为，在系统受到危害前发出警告，防患于未然。

第7章：介绍代理和日志清除技术，此为黑客入侵常用的隐藏和清除入侵痕迹的手段。

第8章：介绍几种常见的远程控制技术，通过远程控制，不需要亲自接触用户的计算机也可以对其计算机进行操作，如今在远程教育、远程协助、远程维护等方向应用较多。

第9章：介绍压缩文件、多媒体文件、光盘等几种常见文件类型的加密解密技术以及几种常用的加密解密工具。

第10章：介绍常见的网络欺骗方式与安全防范方法，并且对支付宝、财付通

等网络支付工具安全防护进行讲解。

第 11 章：介绍 SQL 注入、PHP 注入等常见网站攻击手法并给出了预防措施。

第 12 章：介绍 QQ 账号盗取方式以及防御手法。

第 13 章：介绍系统和数据的备份与恢复，在系统遭受木马病毒攻击而无法使用时，备份与恢复就能够发挥作用。

第 14 章：介绍间谍软件的清除和系统清理，保证系统环境更加安全。

本书特色如下：

- 简单易懂。本书内容从零起步，由浅入深，适合初步接触黑客攻防技术的用户。
- 实用性强。本书理论和实例相结合，并配以大量插图，步骤解释明晰，让读者能够一目了然，轻松学习。
- 有许多小技巧和小窍门。帮读者答疑解惑，提高学习效率。

本书语言简练，内容丰富，并配有大量操作实例，综合作者使用经验和操作心得，可以作为个人学习和了解黑客攻防知识的参考书籍。

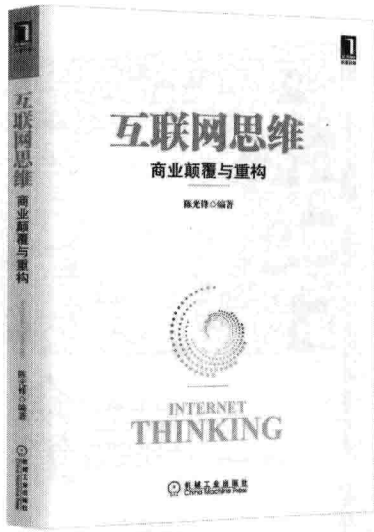
感谢广大读者的阅读与支持，由于作者水平有限，书中难免存在疏漏之处，欢迎批评指正。

本书主要由王叶和李瑞华编写，其他参与编写和资料整理的人有李虹、苏桂兰、安美兰、孟永、黄凌云、杨若、杨爱东、连军峰、陈艳华、杨雪霞、林强、汪强、李晓华、肖聪、多国华。

作者

2014 年 4 月

推荐阅读



互联网思维

第1本系统化阐述互联网思维的力作！

深度揭秘12大核心互联网思维！

瞬间掌握互联网思维精髓！

即刻改变未来=一本可以影响个人与企业命运的著作！

本书以雷军互联网七字诀“专注、极致、口碑、快”为核心精髓，结合马化腾在腾讯15周年 “WE大会”上发表的“马七条”讲话精神，系统化提炼出互联网12大核心思维：标签思维、简约思维、NO.1思维、产品思维、痛点思维、尖叫点思维、屌丝思维、粉丝思维、爆点思维、迭代思维、流量思维、整合思维。

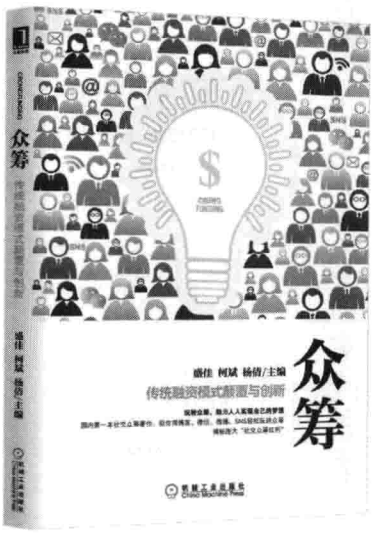
本书产品经理可以读读，从而认识对于产品来说，以哪些为产品素质的考核，又需要对产品做出怎样的调整；数据如何进行解读，又有哪些数据能够帮助我们认识用户的要求；如何在产品的制作中深挖用户的“痛点”，又如何利用“快速迭代”来完成产品的焕然一新。

运营经理也可以读读，在粉丝经济时代，粉丝只是一弯水中月，看得到捞不着。如何把握粉丝的参与感，又如何在恰当的时候激励粉丝，保持敏感的思维和触觉，随时感知到可能存在的引爆点，互联网思维的运营应该往这个方向去。

企业管理者也可以读读，关于如何提高产品的水平，同时又能有效避免人力成本和时间成本的浪费，在KPI和ROI的结合下，实现最大的效益。通过行业上下游合作，提高自身产品的能力，又如何将企业资源整合，成为产业链中不可或缺的平台。

本书是企业成长的必备参考书，适合每一位致力于企业快速成长及提升自身综合实力的职场人士阅读，对初创企业、在互联网方面涉足不深，以及处在发展缓慢状态的公司都有极大的启示作用。

推荐阅读



众筹

国内第一本社交众筹著作：教你用博客、微信、微博、SNS轻松玩转众筹，揭秘庞大“社交众筹红利”

未来属于众筹。十年内，众筹在全球将有3000亿美元的市场规模。

本书站在市场最前沿，回眸众筹历史，描述众筹的当下图景，理性分析众筹模式的革命性，勾勒出在社交网站上玩转众筹的模式，并深入解读中美众筹业不同的发展机遇与监管规则，解密推动众筹成为主流筹资方式的动力所在。

本书适合希望在互联网金融新浪潮中所斩获的读者，是低收入群体、初始创业者、梦想家及中小微企业通过互联网融资方式找到机遇、迅速成长的必备金融服务读本。

目录

第2章 信息的扫描与嗅探 / 33

第3章 系统漏洞入侵与防范 / 72

第4章 病毒入侵与防御 / 92

第5章 木马入侵与防御 / 114

第1章 从零开始认识黑客

想要学习黑客知识，就得了解 IP 地址、端口以及黑客常见的术语及命令。本章正是针对初学者对这方面了解不多，专门做出讲解，从而帮助读者为后面的学习打好基础。

主要内容：

- 认识黑客
- 认识 IP 地址
- 认识端口
- 黑客常见术语与命令
- 在计算机中创建虚拟测试环境

1.1 认识黑客

1.1.1 白帽、灰帽和黑帽黑客

自 1994 年以来，因特网在全球的迅猛发展为人们提供了方便、自由和无限的财富，政治、军事、经济、科技、教育、文化等各个方面都越来越网络化，网络逐渐成为人们生活、娱乐的一部分。可以说，信息时代已经到来，信息已成为物质和能量以外维持人类社会的第三资源，它是未来生活中的重要介质。随着计算机的普及和因特网技术的迅速发展，黑客也随之出现。

黑客的基本含义是指熟练掌握电脑技术的人，但大部分的媒体将“黑客”用于指代电脑侵入者。

白帽黑客是指有能力破坏电脑安全但不具恶意目的的黑客。白帽子一般有清楚的定义、道德规范并常常试图同企业合作去改善发现的安全弱点。

灰帽黑客是指对于伦理和法律态度不明确的黑客。

黑帽黑客经常用来区别于一般（正面的）理性的黑客。这个词自 1983 年开始流行，大概是由于采用了音译，结合 safe cracker 的含义，化为一个犯罪和黑客的合成词。

1.1.2 黑客、红客、蓝客和骇客

黑客，最早源自英文 hacker，他们都是水平高超的电脑专家，尤其是程序设计人员，是一个统称。

红客，维护国家利益，代表中国人民意志，他们热爱自己的祖国、热爱民族、热爱和平，极力维护国家安全与尊严。

蓝客，信仰自由，提倡爱国主义，用自己的力量来维护网络的和平。

骇客，是 cracker 的音译，就是“破解者”的意思，从事恶意破解商业软件、恶意入侵他人的网站等事务。

1.2 认识 IP 地址

在网络上，只要利用 IP 地址就可以找到目标主机，因此，如果要攻击某个网络主机，就要先确定该目标主机的域名或 IP 地址。

1.2.1 IP 地址概述

所谓 IP 地址就是一种主机编址方式，给每个连接在 Internet 上的主机分配一个 32bit 的

地址，也称为网际协议地址。

按照TCP/IP（Transport Control Protocol/Internet Protocol，传输控制协议/Internet协议）协议族的规定，IP地址用二进制来表示，每个IP地址长32bit，换算成字节就是4字节（Byte）。例如，一个采用二进制形式的IP地址是“00001010000000000000000000000001”，这么长的地址处理起来就会很费劲，为了方便使用，IP地址经常被写成十进制的形式，中间使用符号“.”分隔不同的字节，即用XXX.XXX.XXX.XXX的形式来表现，每组XXX代表小于等于255的十进制数，例如192.168.38.6。IP地址的这种表示方法称为“点分十进制表示法”，这显然比二进制的1或0容易记忆多了。

一个完整的IP地址信息，通常应包括IP地址、子网掩码、默认网关和DNS 4部分内容。它们4个只有协同工作时，用户才可以访问Internet并被Internet中的计算机所访问（采用静态IP地址接入Internet时，ISP应当为用户提供全部IP地址信息）。

1. IP地址

企业网络使用的合法IP地址，由提供Internet接入的服务商（ISP）分配私有IP地址，私有IP地址则可以由网络管理员自由分配。但网络内部所有计算机的IP地址都不能相同，否则，会发生IP地址冲突，导致网络连接失败。

2. 子网掩码

子网掩码是与IP地址结合使用的一种技术，其主要作用有两个：一是用于确定地址中的网络号和主机号，二是用于将一个大的IP网络划分为若干个小子网络。

3. 默认网关

当一台主机找不到可用的网关时，就把数据包发送给指定的默认网关，由这个网关来处理数据包。从一个网络向另一个网络发送信息，也必须经过一道“关口”，这道关口就是网关。

4. DNS

DNS服务用于将用户的域名请求转换为IP地址。如果企业网络没有提供DNS服务，则DNS服务器的IP地址应当是ISP的DNS服务器。如果企业网络自己提供了DNS服务，则DNS服务器的IP地址就是内部DNS服务器的IP地址。

1.2.2 IP地址的分类

在互联网中的每个接口有一个唯一的IP地址与其对应，该地址并不是采用平面形式的地址空间，而是具有一定的结构。一般情况下，IP地址可以分为5大类：A类、B类、C类、D类及E类。

这些32位的地址通常写成4个十进制数，其中每个整数对应一个字节。这种表示方法称做“点分十进制表示法（Dotted Decimal Notation）”。