宝典丛书

100万

# 网络安全与黑客攻防宝典

普及安全知识，深入分析黑客入侵的全部过程，剖析病毒和木马的来龙去脉

将基本理论与实践技巧融入到范例中，全面覆盖网络安全与黑客攻防的各种知识及应对技巧

以基础知识为主，同时吸纳大量如Metasploit、UTM、网络钓鱼和NetS-tumbler等新知识

张庆华　编著

電子工業出版社
Publishing House of Electronics Industry
http://www.phei.com.cn

宝 典 丛 书

# 网络安全与黑客攻防宝典

张庆华　编著

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

## 内 容 简 介

本书由浅入深、循序渐进地介绍了计算机网络安全的知识体系。全书共分 14 章，内容涵盖了网络的基础知识、黑客初步、操作系统漏洞与应用软件漏洞的攻防、BBS 与 Blog 的漏洞分析、信息收集、扫描目标、渗透测试、网络设备的攻击与防范、木马分析、病毒分析、防火墙技术、入侵检测技术、计算机取证、无线网络安全等内容。本书最大的特色在于知识全面、实例丰富，每一节的例子都是经过精挑细选，具有很强的针对性，读者可以通过亲手实践而掌握安全防护基本要领和技巧。

本书适合初、中级用户学习网络安全知识时使用，同时也可作为高级安全工程师的参考资料。



**图书在版编目(CIP)数据**

网络安全与黑客攻防宝典 / 张庆华编著.—北京：电子工业出版社，2007.4
（宝典丛书）
ISBN 978-7-121-04142-6

Ⅰ. 网… Ⅱ.张… 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（2007）第 041212 号

责任编辑：于 兰
印　　刷：北京市天竺颖华印刷厂
装　　订：三河金马印装有限公司
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：787×1092　1/16　　印张：44　　字数：1253 千字
印　　次：2007 年 4 月第 1 次印刷
定　　价：78.00 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，联系电话：（010）68279077；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到 dbqq@phei.com.cn。

服务热线：（010）88258888。

# 前　言

在当今的网络时代，黑客、病毒让人们谈虎色变，那么到底什么是黑客，他们如何工作，病毒到底是什么，病毒的出现又会对人们的生活造成什么样的影响？本书将给出这些问题的答案。

计算机网络安全是现今网络的主旋律，关于网络安全的话题在媒体上随处可见。随着黑客工具的日益“傻瓜”化，黑客已经被剥离了神秘的外衣。但是计算机安全、网络安全知识的普及仍然是一个严峻的问题，为了解决这个问题，本书以普及安全知识为己任，帮助用户深入了解网络安全的方方面面，如将深入分析黑客入侵计算机的全部过程，模仿黑客入侵计算机并提升远程计算机的权限进而达到控制的目的，剖析病毒和木马的来龙去脉，预测入侵检测的技术发展及趋势，此外，神秘的计算机取证技术和热点的无线网络安全问题都将在本书中呈现。

本书依照读者的学习规律，首先从了解网络安全的基础知识讲起，介绍基本概念和基本观点，在读者掌握了这些基本知识的基础上，再介绍历史上著名的黑客人物及历史事件，以立体的角度、有趣的故事情节为依托，严格遵循由浅入深、循序渐进的原则。本书以计算机网络安全知识的层次结构为主线将各种工具、命令和理论知识交织编排在一起，使读者可以深入学习任何一章的内容。

本书在内容编排和目录组织上都十分讲究，章节之间既可相互呼应也可各自成章。比如在第 1 章熟悉了网络的基础知识以后，立刻引入一些著名的黑客人物的经历，以一个实例告诉读者这些知识的重要性，让读者在茶余饭后的闲谈中即可快速入门。同时，每章之间又相互独立，如果读者希望直接了解病毒的相关知识，可快速查阅第 9 章和第 10 章。第 9 章对木马进行了深入的分析，第 10 章按照病毒的机制对病毒进行了深入的剖析。

和其他书籍相比，本书具有以下特点：

- **内容丰富，实例经典。**
  在学习计算机网络安全知识时，经常遇到两种情况，一是单纯地讲理论而对知识实践只字不提；另外就是纯粹讲解实战而对涉及的理论不予理会。本书则不同，本书追求理论与实践的结合，使用浅显的语言尽可能地通过精心设计的经典实例，将计算机网络安全的基本理论和实践技巧融入到范例当中，全面覆盖计算机网络安全的各个角落。
- **实战众多，内容充实。**
  作者在讲解每一个知识点之后，都要安排尽可能多的实例。这些实例都是根据实战经验改编，充分考虑了读者的理解水平，并且实战的每一步都介绍得非常详细，读者能够根据自身的知识水平有针对性地学习，思路变得更加开拓。
- **讲解通俗，步骤详细。**
  每个实例的演练步骤都以通俗易懂的语言阐述，并穿插说明文字，还附加了详细的插图作为演练的参考。
- **知识面开阔，重点突出。**
  本书涉及的内容众多，有基础知识，也有深入的理论探讨。为了说明某一个知识点，

在前面使用了一些基础知识作为铺垫，这些知识既可作为了解的必要步骤，也可作为参考知识供读者查阅。

- **新知识多，讲解全面。**

  在本书中使用了大量的新知识，如 Metasploit、Nessus、UTM、EnCase、网络钓鱼、流氓软件和 NetStumbler 等。这些新知识的使用充实了本书的内容，也使得本书与同类书中陈旧的技术内容形成了鲜明的差别。本书不仅介绍了新知识，而且针对这些知识进行实战演练，帮助读者快速了解新内容。

- **实例鲜活，应用软件可随时获得。**

  虽然本书中使用了大量软件，但是这些软件基本上都是免费软件，读者可以从网络上随时下载进行练习，这就避免了读者只能阅读，不能实战的尴尬。

- **兼顾各个水平的读者。**

  虽然本书面向基础读者，但是本书中也介绍了很多理论知识，这些内容可以为高级读者进一步参考。

本书包括以下内容：

**第 1 章** 首先介绍网络的基本体系构成、网络的工作原理、黑客的基本知识、常用的端口知识，以及一般性的安全防范知识。

**第 2 章** 切入正题，介绍黑客的一些情况，如历史上的著名黑客及其参与的事件、著名的黑客组织、黑客通常使用的入侵手法和这些手法的防范方法等。

**第 3 章** 以操作系统常见的漏洞为主题，介绍如何利用这些漏洞入侵远程计算机的过程，并给出了防范方法。另外，还介绍了服务器软件的一些漏洞及其解决方法。

**第 4 章** 继续第 3 章重点分析 BBS 系统和 Blog 系统的一些问题，如提升权限、Cookies 问题及数据库暴库的问题。

**第 5 章** 帮助读者了解高级的黑客搜集信息工具及方法，如使用 Google 搜集网站信息、DNS 查询和追踪路由等知识。

**第 6 章** 主要介绍各种扫描技术及技巧，如 SYN 扫描、圣诞树扫描、FIN 扫描、空扫描、UDP 扫描等，还介绍了操作系统协议栈指纹识别技术。这一章使用了各种著名的扫描器，并给出了实战分析。

**第 7 章** 介绍黑客入侵的高级知识及渗透测试。其中重点介绍了一些渗透测试的基础知识和测试过程中涉及的技术问题，如分析缓冲区溢出问题及各种溢出知识，还介绍了数据库及 Web 渗透的基本技术，并在最后演示了一种在国外非常流行的测试工具平台 Metasploit 的使用方法。

**第 8 章** 介绍网络设备的基本知识，如路由器和交换机的工作原理，以及一些常用的网络设备攻击方法，如使用 SNMP 对路由器入侵及 TFTP 的使用方法。

**第 9 章** 从各个角度对木马进行了深入剖析。其中涉及木马的基本概念、木马常用攻击手段、木马程序的隐藏技术、木马攻击的防范与清除；介绍一些典型木马，如灰鸽子、冰河、RAdmin 的基本知识；还介绍了使用冰刃检查木马进程及 Ethereal 防范木马的一些方法和技巧。

**第 10 章** 介绍从病毒基本知识、病毒分析、病毒类型、新型病毒分析、各种操作系统病毒等方面介绍计算机病毒相关知识。

**第 11 章** 介绍防火墙的基本功能、工作原理、分类、体系结构、规则，随后介绍如何选择

合适的防火墙和部分防火墙产品，在此基础上详细介绍了在不同操作系统平台下的防火墙软件的使用方法。

**第 12 章** 首先概述 IDS 的功能与模型、基本原理等，随后介绍产品选型原则及部分产品，然后着重介绍开源入侵检测系统 Snort，最后还阐述了入侵防御系统与 UTM 等未来发展方向。

**第 13 章** 介绍计算机取证的相关知识。计算机取证将计算机系统视为犯罪现场，运用先进的技术工具，按照规程全面检查计算机系统，提取、保护并分析与计算机犯罪相关的证据，以期据此提起诉讼。这一章从证据的获取和证据的分析两个方面结合相应软件进行了介绍。

**第 14 章** 介绍无线网络安全的内容，其中对无线访问设备、AP、无线网络协议、WEP 安全协议、NetStumbler 检测无线网络、无线网络的攻击及防护无线网络等知识进行了浅显的阐述。

本书具有知识全面、实例精彩、指导性强的特点，力求以全面的知识性及丰富的实例来指导读者透彻学习计算机网络安全技术。本书可以作为对计算机网络安全感兴趣的读者的启蒙书，也可以帮助具有一定技术程度的中级读者提高技能，对高级读者也有一定的启发意义。

本书由张庆华主编，参加本书编写工作的人员还有杨光景、杨毅、李海涛、汪洋、谷文港、陈亮、李守军、江旭初、王坤、赵元、易福华、易阳华、孙江苏、姜海森、张明霞、王江、王斌、郭剑云、张大发、刘挺、尹海涛、戴隆忠、李善坡、张磊、唐友生、于兆海、刘洪燕、傅翠娇、王悠。在此向他们表示感谢。

作者

2007 年 1 月

# 反侵权盗版声明

# 读者意见调查表

感谢您对电子工业出版社的支持！

为帮助我们进步，请将您的宝贵意见填于下表并寄回我们。

| | |
|---|---|
| 您购买的图书名称 | |
| 先进性和实用性 | □很好 □好 □一般 □不太好 □差 |
| 图书文字可读性 | □很好 □好 □一般 □不太好 □差 |
| 图书篇幅适宜度 | □很合适 □合适 □一般 □不合适 □差 |
| 出版物中差错 | □极少 □较少 □一般 □较多 □太多 |
| 图书封面设计水平 | □很好 □好 □一般 □不太好 □差 |
| 图书印刷装订质量 | □很好 □好 □一般 □不太好 □差 |
| 纸张质量 | □很好 □好 □一般 □不太好 □差 |
| 定价 | □很便宜 □便宜 □合理 □贵 □太贵 |
| 对宣传工作的感觉 | □很好 □好 □一般 □不好 □差 |
| 对服务质量的感觉 | □很好 □好 □一般 □不好 □差 |
| 从何处获取出版物信息 | □书目报 □电子社宣传材料 □书店 □他人转告 □网站 □报刊 |
| 您认为电子工业出版社应改进的方面 | □先进性和实用性 □文字可读性<br>□篇幅适宜度 □出版物中差错<br>□设计水平 □印刷装订质量 □纸张质量（光盘材质）<br>□定价 □宣传工作 □服务质量 |
| 您的具体意见或建议 | |
| 读者姓名： 联系方式：<br>从事工作：□技术研发 □技术管理 □经营管理 □行政管理 □教育培训 □在校学习 | |

表格寄回：邮寄地址：北京市万寿路 173 信箱 邮政编码：100036 收信人：肖 萍

传真：（010）88254300 收件人：同收信人

电子信箱：xiaoping@hxex.cn

# 目　录