宝典丛书 200万

网络安全与黑客攻防（第3版）宝典

作者根据实战经验精心改编的实例将帮助读者借鉴并开拓思路

涉及无线网络、Metasploit、Nessua、UTM、网络钓鱼、流氓软件等最新技术，阅读价值大大提升

全面提供有针对性的防守方案

李俊民　等编著

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

（第3版）

李俊民　等编著

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 21 章，内容涵盖网络的基础知识、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、网络脚本攻防、SQL 注入攻防、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，每一节的例子都经过精挑细选，具有很强的针对性，读者可以通过亲手实践进而掌握安全防护的基本要领和技巧。

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 / 李俊民 等编著.—3 版. —北京：电子工业出版社，2011.5
（宝典丛书）
ISBN 978-7-121-13124-0

Ⅰ. ①网… Ⅱ. ①李… 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(2011)第 044830 号

责任编辑：张月萍
印　　刷：北京东光印刷厂
装　　订：三河市皇庄路通装订厂
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：49.25　　字数：1386千字
印　　次：2011年5月第1次印刷
印　　数：4000册
定　　价：89.00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，如深入分析黑客入侵计算机的全过程，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系统的目的，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。

本书特色

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；二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，使思路变得更加开拓。

- **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。**
  在本书中介绍了大量的新知识，如 Metasploit、Nessus、UTM、EnCase、网络钓鱼、流氓软件和 NetStumbler 等。这些新知识的介绍充实了本书的内容，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。
- **兼顾各种水平的读者。**
  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，这些内容可为高级读者提供进一步参考。

本书内容

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 帮助读者了解高级黑客搜集信息的工具及方法，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　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　用户在使用网络资源时，需要了解针对各种计算机病毒和木马的防范方法。本章介绍了这些方法。

第 12 章　脚本攻击通常针对这些数据库来配合脚本对一些变量的过滤不严等问题，得到用户密码等敏感信息。本章就教会我们如何摆脱脚本攻击。

第 13 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 14 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 15 章　让用户学习通过对网络的封锁和代理突破，来实现维护计算机网络的安全性和可靠性。

第 16 章　讲解针对计算机操作系统的攻防技术，以及如何实现对软件和文件资料进行加密等相关的内容。

第 17 章　讲解 ASP 和 PHP 环境下的 SQL 注入技术，并了解 SQL 注入的防护。

第 18 章　讲解在计算机网络安全的攻防中，使用欺骗攻击技术实施攻击的原理及其安全防范方面的相关知识。

第 19 章　讲解与后门技术相关的一些内容，使得读者对后门技术的攻击及防范知识有一定的了解。

第 20 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 21 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。

本书作者

本书主要由李俊民编写。其他参与编写的人员有张金霞、于锋、张伟、曾广平、刘海峰、刘涛、赵宝永、郑莲华、张涛、杨强、陈涛、罗渊文、李居英、郭永胜。在此对所有参与编写的人表示感谢！

由于笔者水平所限，书中可能还存在疏漏和错误，还望广大读者批评指正。

严 正 声 明

严正声明：本书所讨论的技术仅用于研究学习，旨在最大限度地唤醒大家的信息安全意识，提高信息安全防护技能，严禁用于非法活动。任何个人、团体、组织不得将其用于非法目的，违法犯罪必将受到法律的严厉制裁。

《中华人民共和国刑法》关于信息安全的条例

第二百五十三条之一 国家机关或者金融、电信、交通、教育、医疗等单位的工作人员，违反国家规定，将本单位在履行职责或者提供服务过程中获得的公民个人信息，出售或者非法提供给他人，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金。

第二百八十五条 违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。

违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的，依照前款的规定处罚。

第二百八十六条 违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。

违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。

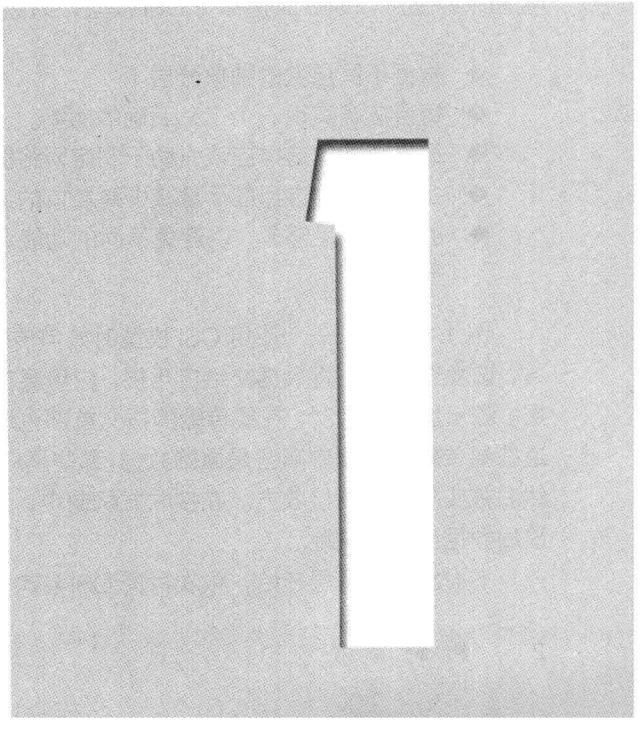
故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。

第二百八十七条 利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的，依照本法有关规定定罪处罚。

目　录

Part 1

第1部分　黑客基础篇



第 1 章　网络基础知识

本章包括

- ◆ISO 提出的 OSI 模型
- ◆网络的 TCP/IP 协议基础
- ◆域名系统、DHCP、NetBIOS 及 SMB 的简单知识
- ◆计算机端口的基础知识
- ◆计算机安全分析工具的简单介绍

进入 21 世纪之后，网络已经成为人们生活中不可或缺的获取信息的重要手段。截至 2009 年 6 月 30 日，根据 CNNIC（中国互联网络信息中心）的《第 24 次中国互联网络发展状况统计报告》，中国网民人数已经突破 3.38 亿。人们对网络的使用越来越频繁，网民平均每周上网 30 小时，达到了新的历史高度。对于办公室人员来说，每天上班的第一件事就是打开浏览器在新浪、搜狐、网易等主要网络新闻媒体上浏览当天的新闻，网络的力量可见一斑。

21 世纪的网络发展最主要的特点是计算机与通信的结合，这种方式对计算机的普及产生了深远的影响。依赖网线将多台分散的计算机互连起来使之成为共享模式即被称为计算机网络，而将这些计算机网络连接起来就形成了国际网络的模式，即互联网。

1.1　OSI 模型

OSI 模型是由国际标准化组织（ISO）提出的，它作为将各层上使用的协议国际标准化的第一步发展起来，这一模型被称为 ISO OSI 开放系统互联参考模型，因为这是关于如何把开放式系统连接起来的模型，故被简化称为 OSI 模型，如图 1.1 所示。OSI 模型有 7 层，其分层原理如下：

- ◆ 根据不同层次的抽象分层。
- ◆ 每层应当实现一个定义明确的功能。
- ◆ 每层功能的选择应该有助于制定网络协议的国际标准。
- ◆ 各层边界的选择应尽量减少跨接口的通信量。
- ◆ 层数应该足够多，以避免不同的功能混杂在同一层中，但也不能太多，否则体系结构会过于庞大。

图 1.1 演示了一个使用 OSI 模型时如何传输数据的例子。发送进程中有些数据需要发送给接收方，该发送方首先将数据交给应用层，应用层在此基础上增加一个应用报文头，再将结果交给表示层。表示层如法炮制，在要传输的报文首部也增加一个报文头。但是需要注意的是，表示层并不知道在要传输的数据中哪些是原始数据，哪些是应用报文头。这个过程重复进行直到数据抵达物理层，然后被实际传输到接收方。在接收方机制中，当信息向上传递时，各种报文头被一层一层地剥去，最后数据到达目的地。

下面将从物理层开始，依次讨论 OSI 参考模型中各层的功能和作用。