高等院校信息安全专业规划教材

黑客攻防技术与实践

- 信息收集的常用方法及使用工具
- 常见网络攻击的基本原理与常用工具
- 边界网关（防火墙、VPN）的基本原理及操作实例
- windows 系统安全的基本原理及操作实例
- 病毒与木马的基本常识和防范方法

提供电子教案

李建华　主编
单蓉胜　李昀　陈楠　参编

机械工业出版社
CHINA MACHINE PRESS

高等院校信息安全专业规划教材

黑客攻防技术与实践

主编　李建华
参编　单蓉胜　李　昀　陈　楠

机械工业出版社

本书介绍了信息安全攻防技术的基本原理和实现工具。全书共分18章，既介绍了网络攻击技术，如信息搜集、拒绝服务攻击、网络嗅探、欺骗与会话劫持、Web攻击、密码破解、病毒、蠕虫与木马、后门技术和踪迹隐藏等攻击技术，也详细分析了防火墙、入侵检测技术、数据保护、Windows系统安全、Web安全等技术，还介绍了攻击技术和防御技术的实践操作实例。

本书既可以作为高等学校信息安全课程的教材，也适合企事业单位的网络管理员、系统管理员等专业技术人员作为工作学习和参考。

图书在版编目（CIP）数据

黑客攻防技术与实践/李建华主编. —北京：机械工业出版社，2009.4
（高等院校信息安全专业规划教材）
ISBN 978-7-111-26785-0

Ⅰ.黑… Ⅱ.李… Ⅲ.计算机网络-安全技术-高等学校-教材
Ⅳ.TP393.08

中国版本图书馆CIP数据核字（2009）第052447号

机械工业出版社（北京市百万庄大街22号 邮政编码 100037）
责任编辑：唐德凯
责任印制：乔 宇
北京双青印刷厂印刷

2009年7月第1版·第1次印刷
184mm×260mm·23.5印张·580千字
0001—3000册
标准书号：ISBN 978-7-111-26785-0
定价：39.00元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
销售服务热线电话：（010）68326294 68993821
购书热线电话：（010）88379639 88379641 88379643
编辑热线电话：（010）88379753 88379739

高等院校信息安全专业规划教材

编委会成员名单

出版说明

信息技术的发展和推广，为人类开辟了一个新的生活空间，它正对世界范围内的经济、政治、科教及社会发展各方面产生重大的影响。如何建设安全的网络空间，已成为一个迫切需要人们研究、解决的问题。目前，与此相关的新技术、新方法不断涌现，社会也更加需要这类专门人才。为了适应对信息安全人才的需求，我国许多高等院校已相继开设了信息安全专业。为了配合相关的教材建设，机械工业出版社邀请了解放军信息工程大学、解放军理工大学通信工程学院、上海交通大学、西安电子科技大学、湖南大学、中山大学、南京邮电学院等高校的专家和学者，成立了教材编委会，共同策划了这套面向高校信息安全专业的教材。

本套教材的特色：

1. 作者队伍强。本套教材的作者都是全国各院校从事一线教学的知名教师和学术带头人，具有很高的知名度和权威性，保证了本套教材的水平和质量。

2. 系列性强。整套教材根据信息安全专业的课程设置规划，内容尽量涉及该领域的方方面面。

3. 系统性强。能够满足专业教学需要，内容涵盖该课程的知识体系。

4. 注重理论性和实践性。按照教材的编写模式编写，在注重理论教学的同时注意理论与实践的结合，使学生能在更大范围内、更高层面上掌握技术，学以致用。

5. 内容新。能反映出信息安全领域的最新技术和发展方向。

本套教材可作为信息安全、计算机等专业的教学用书，同时也可以供从事信息安全工作的科技人员以及相关专业的研究生参考。

机械工业出版社

前　言

伴随电子商务、电子政务的全面铺开，信息安全行业面对的将是一场前所未有的机遇和挑战。由于信息网络的开放性和复杂性，安全保障的各个状态都处于一种不稳定的快速变化过程中。安全保障的各个环节，如风险评估，威胁监测与分析、事件发现、事件控制甚至系统恢复与生存等，都需要具备足够的动态适应能力，以便适应各种变化的状况。然而，如何达到这个要求也面临大量的技术挑战。

黑客攻防技术是伴随着 Internet 的快速延伸而不断发展和完善的技术体系。本书以信息攻防的一对矛盾体为线索为读者逐一展开黑客技术体系的全貌，分为攻击技术、防御技术、攻防实践三个部分，共 18 章。第一部分为黑客攻击技术，涉及九个方面的攻击类型和方法；第二部分为防御技术，包括防火墙、入侵检测系统、数据保护、Microsoft Windows 系统安全、Web 安全等；第三部分为攻防实践，是上述各种技术的实践环节。本书的特色在于：同时涉及攻击与防御技术，将各种攻防技术系统化；配有专门的实践部分，强化了攻防理论与具体实践的结合。本书可用作大专院校计算机、信息安全等专业的本科生、研究生教材，也适合网络安全技术爱好者自学使用。

本书主编是李建华教授，单蓉胜博士参加了第 12～15 章、18 章的编写并负责统稿工作；李昀博士参加了第 1～5 章、16 章的编写工作；陈楠硕士参加了第 6～11 章、17 章的编写工作。

感谢赵旭东博士生对全书的校对。本书的顺利出版，要感谢上海交通大学信息安全工程学院的领导和老师所给予的大力支持和帮助。

本书作为面向 21 世纪高等院校信息安全技术的教材，体现了信息安全技术课程改革的方向之一。本课程建议授课学时为 40 学时，实验学时为 20 学时，并要求先修计算机网络课程。

由于编著水平有限，书中难免存在不妥之处，敬请读者批评指正。

编　者

目　录

第1章 基础知识

1.1 历史上的十大黑客事件

DNA 杂志在印度全国软件和服务企业协会(Nasscom) 与孟买警方开展互联网安全周活动,并回顾历史上的十大黑客事件时深刻认识到,即使是那些被认为固若金汤的系统在黑客攻击面前也总是显得不堪一击。

20 世纪 90 年代早期,出现了一位在世界范围内举足轻重的黑客——Kevin Mitnick。诺基亚(Nokia),富士通(Fujitsu),摩托罗拉(Motorola)和 Sun Microsystems 等世界上几大科技和电信公司的电脑系统都曾被他"光顾"过。1995 年他被 FBI 逮捕,于 2000 年获得假释。他从来不把自己的这种入侵行为称为黑客行为,按照他的解释,应为"社会工程(Social Engineering)"。

2002 年 11 月,伦敦人 Gary McKinnon 在英国被指控非法侵入美国军方 90 多个电脑系统。

1995 年,来自俄罗斯的黑客 Vladimir Levin 在互联网上上演了精彩的"偷天换日"。他是历史上第一个通过入侵银行电脑系统来获利的黑客。当年,他侵入美国花旗银行并盗走 1000 万美元。之后,他把账户里的钱转移至美国、芬兰、荷兰、德国、爱尔兰等地。

1990 年,为了获得在洛杉矶地区 kiis-fm 电台第 102 个呼入者的奖励——保时捷 944 s2 跑车,Kevin Poulsen 控制了整个地区的电话系统,以确保他是第 102 个呼入者。最终,他如愿以偿地获得了跑车并为此入狱 3 年。他现在是 Wired News 的高级编辑。

1983 年,当 Kevin Poulsen 还是一名学生的时候,他就曾成功入侵 ARPANET(现在使用的 Internet 的前身)。Kevin Poulsen 当时利用了 ARPANET 的一个漏洞,能够暂时控制美国地区的 ARPANET。

1996 年,美国黑客 Timothy Lloyd 曾将一个六行的恶意软件放在了其雇主——Omega 工程公司(美国航天航空局和美国海军最大的供货商)的网络上。整个逻辑炸弹删除了 Omega 工程公司所有负责生产的软件。此事件导致 Omega 工程公司损失 1000 万美金。

1988 年,年仅 23 岁的 Cornell 大学学生 Robert Morris 在 Internet 上释放了世界上首个"蠕虫"程序。Robert Morris 最初仅仅是把他这个 99 行的程序放在互联网上进行试验,可结果却使他的计算机被感染并迅速在互联网上蔓延开,美国等地接入互联网的计算机都受到了影响。Robert Morris 也因此在 1990 年被判入狱。

1999 年,Melissa 病毒是世界上首个具有全球破坏力的病毒。David Smith 在编写此病毒的时候年仅 30 岁。Melissa 病毒使世界上 300 多家公司的计算机系统崩溃。整个病毒造成的损失接近 4 亿美金。David Smith 随后被判处 5 年徒刑。

2000 年 2 月 6 ~ 14 日期间,年仅 15 岁的 MafiaBoy(由于年龄太小,因此没有公布其真实身份)成功侵入包括 eBay、Amazon 和 Yahoo 在内的大型网站服务器,他成功阻止了服务器向用户提供服务。同年 MafiaBoy 被捕。

1993 年,自称为骗局大师(MOD)的组织,将目标锁定美国电话系统。这个组织成功入侵