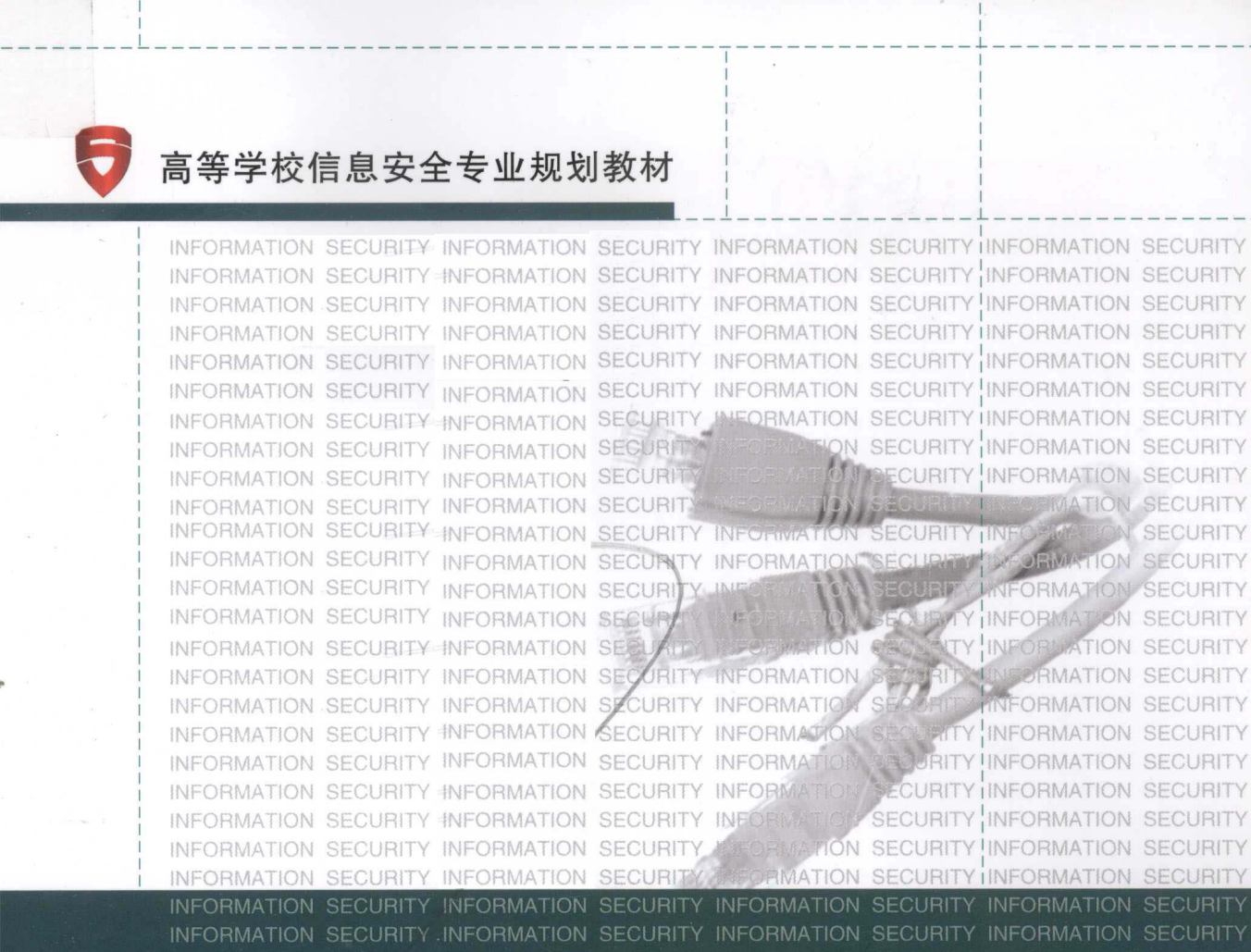
高等学校信息安全专业规划教材



网络攻防技术教程

第二版

杜　晔　张大伟　范艳芳　编著

WUHAN UNIVERSITY PRESS
武汉大学出版社

高等学校信息安全专业规划教材

网络攻防技术教程

第二版

杜 晔 张大伟 范艳芳 编著

WUHAN UNIVERSITY PRESS
武汉大学出版社

图书在版编目(CIP)数据

网络攻防技术教程/杜晔,张大伟,范艳芳编著. —2 版. —武汉:武汉大学出版社,2012.8

高等学校信息安全专业规划教材

ISBN 978-7-307-09956-2

Ⅰ.网… Ⅱ.①杜… ②张… ③范… 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(2012)第 138963 号

责任编辑:林 莉 责任校对:黄添生 版式设计:支 笛

出版发行:**武汉大学出版社** (430072 武昌 珞珈山)

(电子邮件:cbs22@whu.edu.cn 网址:www.wdp.com.cn)

印刷:武汉中科兴业印务有限公司

开本:787×1092 1/16 印张:23 字数:576 千字

版次:2008 年 6 月第 1 版 2012 年 8 月第 2 版

2012 年 8 月第 2 版第 1 次印刷

ISBN 978-7-307-09956-2/TP·436 定价:39.00 元

高等学校信息安全专业规划教材
编　委　会

内容提要

本书详细地介绍了计算机及网络系统面临的威胁与黑客攻击方法，详尽、具体地披露了攻击技术的真相，以及防范策略和技术实现措施。全书理论联系实际，在每部分技术讨论之后，都有一套详细的实验方案对相关技术进行验证。

全书共分四个部分，内容由浅入深，按照黑客攻击通常采用的步骤进行组织，分技术专题进行讨论。第一部分介绍了网络攻防基础知识，以使读者建立起网络攻防的基本概念。第二部分介绍信息收集技术，即攻击前的“踩点”，包括网络嗅探和漏洞扫描技术。第三部分是本书的核心内容，介绍了代表性的网络攻击技术，以及针对性的防御技术。第四部分着重于防御技术，讨论了 PKI 网络安全协议和两种得到广泛应用的安全设备，即防火墙和入侵检测系统。

本书可作为信息安全、计算机、通信等专业本科生、硕士研究生的教科书，也适合于网络管理人员、安全维护人员和相关技术人员参考和阅读。

序 言

二十一世纪是信息的时代，信息成为一种重要的战略资源。信息科学成为最活跃的学科领域之一，信息技术改变着人们的生活和工作方式，信息产业成为世界第一大产业。信息的安全保障能力成为一个国家综合国力的重要组成部分。

当前，以 Internet 为代表的计算机网络的迅速发展和“电子政务”、“电子商务”等信息系统的广泛应用，正引起社会和经济的深刻变革，为网络安全和信息安全开拓了新的服务空间。

世界主要工业化国家中每年因利用计算机犯罪所造成的经济损失远远超过普通经济犯罪。内外不法分子互相勾结侵害计算机系统，已成为危害计算机信息安全的普遍性、多发性事件。计算机病毒已对计算机系统的安全构成极大的威胁。社会的信息化导致新的军事革命，信息战、网络战成为新的作战形式。

总之，随着计算机在军事、政治、金融、商业等部门的广泛应用，社会对计算机的依赖越来越大，如果计算机系统的安全受到破坏将导致社会的混乱并造成巨大损失。因此，确保计算机系统的安全已成为世人关注的社会问题和计算机科学的热点研究课题。

信息安全事关国家安全，事关经济发展，必须采取措施确保我国的信息安全。

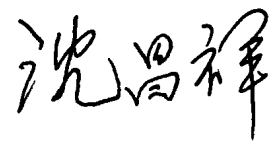
发展信息安全技术与产业，人才是关键。培养信息安全领域的专业人才，成为当务之急。2001 年经教育部批准，武汉大学创建了全国第一个信息安全本科专业。2003 年经国务院学位办批准武汉大学建立信息安全博士点。现在，全国设立信息安全本科专业的高等院校已增加到 70 多所，设立信息安全博士点的高等院校和科研院所也增加了很多。2007 年“教育部高等学校信息安全类专业教学指导委员会”正式成立，并在武汉大学成功地召开了“第一届中国信息安全学科建设与人才培养研讨会”。我国信息安全学科建设与人才培养进入蓬勃发展阶段。

为了增进信息安全领域的学术交流、为信息安全专业的大学生提供一套适用的教材，2003 年武汉大学组织编写了一套《信息安全技术与教材系列丛书》。这套丛书涵盖了信息安全的主要专业领域，既可用做本科生的教材，又可作为工程技术人员的技术参考书。这套丛书出版后得到了广泛的应用，深受广大读者的厚爱，为传播信息安全知识发挥了重要作用。现在，为了能够反映信息安全技术的新进展、更加适合信息安全教学的使用和符合信息安全类专业指导性专业规范的要求，武汉大学对原有丛书进行了升版。

我觉得升版后的这套新教材的特点是内容全面、技术新颖、理论联系实际，努力反映信息安全领域的新成果和新技术，符合信息安全类专业指导性专业规范的要求，适合教学使用。在我国信息安全专业人才培养蓬勃发展的今天，这套新教材的出版是非常及时的和十分有益的。

我代表编委会对图书的作者和广大读者表示感谢。欢迎广大读者提出宝贵意见，以便能够进一步修改完善。

中国工程院院士，武汉大学兼职教授



2008年8月28日

前 言

随着计算机和通信技术的飞速发展，网络应用已日益普及，成为人们生活中不可缺少的一部分。截至2007年12月，我国网民总人数已达？亿。电子政务、电子商务得到进一步推广，有大约22.1%的网民进行网络购物或者商业运作，人数规模达到4640万。但在网络服务为我们提供极大便利的同时，对于信息系统的非法入侵和破坏活动也正以惊人的速度在全世界蔓延，同时带来巨大的经济损失和安全威胁。据统计，每年全球因安全问题导致的损失已经可以用万亿美元的数量级来计算。在我国，“震荡波”系列蠕虫曾造成有超过138万个IP地址的主机被感染的记录，而2007年亦有约4.5万个IP地址的主机被植入木马。

面对如此不容乐观的网络环境和严峻的挑战，无论是网络管理人员还是个人，都应掌握基本的网络攻防技术，做好自身防范，增强抵御黑客攻击的能力。

“知己知彼，百战不殆。”要想防，首先要知道如何攻。本书总结了目前网络攻击现状与发展趋势，详细地介绍了计算机及网络系统面临的威胁和黑客攻击方法，详尽、具体地披露了攻击技术的真相，以及防范策略和技术实现措施。作者采用尽可能简单的方式向读者讲解技术原理，希望读者在读完这本书后，能对网络攻防的技术有进一步的了解。

本书的特点在于理论联系实际。在技术讨论之后，都有一套详细的试验方案对相关技术进行验证。通过具体的试验操作，帮助读者实际掌握和理解各个知识点的精髓。考虑到不同单位千差万别的试验条件，我们的试验内容大部分基于很容易搭建的Windows和Linux操作系统，充分降低了试验开设过程的成本。

本书共分四个部分，内容由浅入深，按照黑客攻击通常采用的步骤进行组织，分技术专题进行讨论。

第一部分介绍了网络攻防基础知识，以使读者建立起网络攻防的基本概念。第二部分介绍信息收集技术，即攻击前的“踩点”，包括网络嗅探和漏洞扫描技术。第三部分是本书的核心内容，介绍了代表性的网络攻击技术，以及针对性的防御技术。第四部分着重于防御技术，讨论了PKI网络安全协议和两种得到广泛应用的安全设备，即防火墙和入侵检测系统。

对于每个技术专题，都详细制定了实验方案，并对实验的每个步骤进行了演练。使读者学习后可以参照教程进行实际操作，通过实践深入理解技术原理。本书可作为信息安全、计算机、通信等专业本科生、硕士研究生的教科书，也适合于网络管理人员、安全维护人员和相关技术人员参考和阅读。

本书编写的目的是帮助读者了解网络攻防技术与内幕，建立安全意识，增强对黑客攻击的防范能力，绝不是为怀有不良动机的人提供支持，也不承担因为技术被滥用而产生的连带责任。

在本书编写的过程中，参考了互联网上公布的研究论文和相关资料，主要源于各大学、科研机构、安全网站、安全公司以及一些研究网络安全问题的个人，在此向他们对于推动安全技术的发展所做的努力表示感谢。由于资料较多，无法一一注明出处。写作过程中所参考

的这些资料，其原文版权属于原作者，特此声明。

本书第 1、2 章由范艳芳编写，第 9 章由张大伟编写，其余各章由杜晔编写并完成全书统稿。北京交通大学信息安全体系结构中心的李洁原、李程、刘博、李磊、何帆、李明、郝悦等参与了编写工作。本书的编写得到了北京交通大学何永忠、袁中兰、黎妹红，哈尔滨工程大学王桐、郭方方，北京理工大学冯远等多位老师的帮助，在此对他们表示衷心的感谢。

由于作者水平有限，书中难免会出现疏漏，加之网络攻防技术纵深宽广，在内容取舍与编排方面，难免有考虑不周之处，诚请广大读者批评指正。

杜　晔

2012 年 7 月

目 录

第一部分 网络攻击基础知识

第二部分　信息收集技术

第三部分　网络攻击技术

第四部分 防 御 技 术

第一部分 网络攻击基础知识