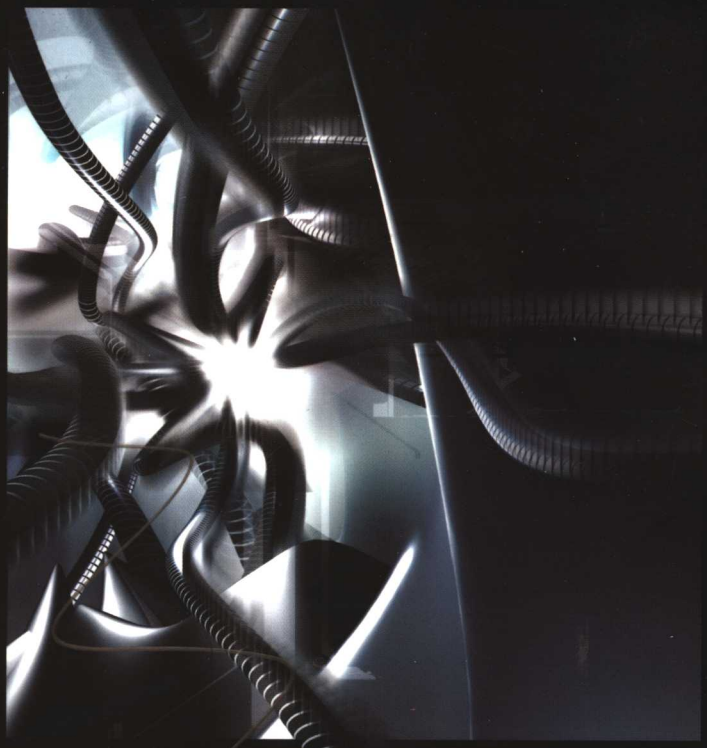
WANGLUO DE
GONGJI YU
FANGFAN
LILUN YU SHIJIAN



网络的攻击与防范
——理论与实践

牛少彰　江为强　编著

北京邮电大学出版社
www.buptpress.com

网络的攻击与防范

——理论与实践

牛少彰　江为强　编著

北京邮电大学出版社
·北京·

内 容 简 介

本书系统论述了网络攻击与防范的原理与技术，并通过大量实践例程加深对内容的理解。本书主要针对 Windows 操作系统，从攻击者和防御者两个方面系统阐述了计算机和网络的入侵手段及相应防范措施。全书共分三篇，18 章，主要包括：网络攻击与防范概论、网络攻击篇和网络防范篇，每章都阐述了其原理、技术及实验，最后对网络安全防范的整体解决方案进行了详细分析。

全书理论与实践相结合，通过实践来理解攻防的具体过程。对所阐述的攻击手段都指出了其危害并提供了防范对策。本书可操作性强，介绍了大量典型的网络攻防工具及操作实例，让读者通过实际操作来掌握相应的原理及技术。

本书可以作为计算机、通信工程、信息安全及相关专业本科高年级学生、研究生的教材和实验或实训用书，也可供从事网络与网络安全工作的工程技术人员及对网络安全技术感兴趣的读者参考。

图书在版编目（CIP）数据

网络的攻击与防范：理论与实践/牛少彰，江为强编著. —北京：北京邮电大学出版社，2006
ISBN 7-5635-1342-6

Ⅰ. 网… Ⅱ. ①牛… ②江… 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（2006）第 129496 号

书　　名：网络的攻击与防范——理论与实践
编　　著：牛少彰　江为强
责任编辑：王晓丹
出版发行：北京邮电大学出版社
社　　址：北京市海淀区西土城路 10 号（邮编：100876）
北方营销中心：电话：010—62282185　传真：010—62283578
南方营销中心：电话：010—62282902　传真：010—62282735
E-mail：publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：北京忠信诚胶印厂
开　　本：787 mm × 960 mm　1/16
印　　张：19
字　　数：413 千字
印　　数：1—3 000 册
版　　次：2006 年 12 月第 1 版　2006 年 12 月第 1 次印刷

ISBN 7-5635-1342-6/TP・259　　定　价：35.00 元（附光盘）

前 言

网络安全是一门综合学科，包括了技术、管理、人才、法律法规诸多方面。从技术的角度重点包含了对攻击手段的分析及其相应的防范措施，安全管理与法律法规是网络安全技术得以实现的有力保障，人才的培养是它的基石。在当前网络安全形势十分严峻的情况下，网络安全人才的缺口越来越大，许多高校都开设了信息安全专业或信息安全课程，相关教材也应运而生。编者深感在信息安全教育中，实践动手能力的培养对其掌握信息安全原理技术起着重要的作用，同时又能快速获得工作中的实际操作经验。目前，研究网络攻击与防范技术的著作很多，但同时对其实践操作进行详细分析的著作不多见。鉴于此，作者根据从事网络安全方面的实验室建设和实训教学的经验，编写了这部理论与实践操作紧密结合的著作，目的是让读者在掌握网络攻击与安全理论的同时，能够通过实际动手操作来加深对攻防原理以及网络攻击的危害和网络防御的重要性的理解。

本书内容全面，既有网络攻防的理论知识，又有其实用技术和实践，并包括网络信息安全方面的一些最新成果。全书共分三篇，18 章。第一篇为网络攻击与防范概论，共 3 章，主要介绍了网络攻击与防范的历史、现状与发展趋势；网络攻击与防范的方法；网络攻击与防范模型；网络安全策略。第二篇为网络攻击篇，共 7 章，按照网络攻击的基本过程，详细介绍了网络攻击的各个阶段以及所使用的手段，并对网络攻击的实施及其原理进行了分析，对所讨论的攻击手段都指出了其危害并提供了防范对策。第三篇为网络防范篇，共 8 章，主要针对第二篇所阐述的攻击手段，介绍了相应的网络防御理论及其在实践中典型的安全技术和产品，包括一些新的安全技术（如蜜罐与蜜网技术等），最后对前述的相关网络安全技术进行归纳，给出了网络安全的整体解决方案。在本书后 2 篇中，每章的后面都有实验或技术解决方案。为了帮助读者更好地理解网络攻击与防范的原理，书中每章后面列出了部分实践的主要步骤，随书所附的光盘中给出了实践的详细的资料及更多的操作实例。

本书最大的特点是理论与实践相结合，通过实践来理解攻防的具体过程。本书

可操作性强，介绍了大量典型的网络攻防工具及操作实例，让读者通过实际操作来掌握相应的原理及技术。

本书可以作为计算机、通信工程、信息安全及相关专业本科高年级学生、研究生的教材和实验用书，特别适合用于信息安全相关专业的实训教学，以及网络攻防的培训教材。本书也可供从事网络与网络安全工作的工程技术人员及对网络安全技术感兴趣的读者参考。

在本书的编写过程中，北京邮电大学的本科毕业生冯浩、冯成晶、张岳、钱进、韦成府、郑直、单艮俊、梁蒙奇、齐麟等为本书收集和整理了大量的材料。研究生丁昆写了部分实验并对所有的实验进行了整理。研究生张丽、化宇鹏、张玮、刘博、向楠、张同庆、卢娜等对书稿进行了大量的校对工作。北京电信教育培训中心的史凤婷老师在实验的组织中做了大量的工作。刘洋、梁凯、王子戈和唐志雄等提供了部分实验内容。本书在编写过程中得到了北京邮电大学信息安全中心和北京电信教育培训中心的大力支持和帮助。在此一并表示衷心感谢

由于本书涉及的内容较多，参考了大量的论文、书籍和网络资源，书后列出了较为详尽的参考文献，但由于参加本书内容收集和整理的人员众多，难免挂一漏万，如有遗漏，敬请谅解。书中的实验部分参考和引用了网络资源，所附软件只是帮助读者学习和理解相应的理论与技术，其著作权属于原作者，请勿用于其他目的，如实际工作中需要使用，请向原作者购买。

限于编者水平有限，书中难免有疏漏和错误之处，恳请读者批评指正。

编者

2006 年 8 月

C O N T E N T S 目录

第一篇 网络攻击与防范概论

第二篇 网络攻击篇

第三篇 网络防范篇

第一篇

网络攻击与防范概论

第 1 章

网络攻击与防范的历史、现状与发展趋势

随着由通信与计算机相结合而诞生的计算机互联网络全面进入千家万户，使得信息共享应用日益广泛与深入。世界范围的信息革命激发了人类历史上最活跃的生产力，人类开始从主要依赖物质和能源的社会步入物质、能源和信息三位一体的社会，信息成为人类社会必须的重要资源。但同时网络的安全问题也日渐突出，而且情况也越来越复杂。从大的方面来说，网络信息安全问题已威胁到国家的政治、经济、军事、文化、意识形态等领域。从小的方面来说，网络信息安全是人们能否保护自己个人隐私的关键。网络信息安全是社会稳定安全的必要前提条件。人们的生活已经无法脱离对网络与计算机的依赖，但是网络是开放的、共享的，因此，网络与计算机系统安全就成为科学研究的一个重大课题。而对网络与计算机安全的研究不能仅限于防御手段，还要从非法获取目标主机的系统信息、非法挖掘系统弱点等技术进行研究。正所谓对症下药，只有了解了攻击者的手法，才能更好地采取措施，来保护网络与计算机系统的正常运行。

1.1 网络与黑客的历史

1.1.1 计算机网络的历史

计算机网络的发展历史不长，但发展速度很快。计算机网络是计算机技术和通信技术紧密结合的产物，它涉及到通信与计算机两个领域。