普通高等教育“十一五”国家级规划教材

高·等·院·校·信·息·安·全·专·业·系·列·教·材

中国计算机学会教育专业委员会与清华大学出版社联合组织编写

名誉主编：何德全　编委会主任：肖国镇

Network Security Lab Manual

网络安全实验教程

刘建伟　张卫东　刘培顺　李晖　编著　　陈克非　审

http://www.tup.com.cn

清华大学出版社

高·等·院·校·信·息·安·全·专·业·系·列·教·材

Network Security Lab Manual

网络安全实验教程

刘建伟 张卫东 刘培顺 李晖 编著 陈克非 审

国家自然科学基金项目资助（批准号：60672102）
国家863计划课题资助（批准号：2006AA01Z422）
总装备部武器装备预研基金项目资助（批准号：9140A21050107HK0114）

清华大学出版社
北京

内 容 简 介

本书内容丰富，实用性强，几乎涵盖了网络安全实验的全部内容，是国内外第一本内容比较全面的信息安全专业实验教材。本书不仅包含了密码学常用算法的实验，同时还包含了大量的网络安全的工具和设备、计算机病毒防护等方面的内容，最主要的是包含了专用的网络安全测试仪器仪表的操作和使用；此外，针对网络安全的发展趋势，本书增加了无线网络安全的实验内容。熟练使用这些工具和设备并进行实验教学，对于提高学生网络安全管理水平，积累网络安全实践经验，具有非常重要的意义。

图书在版编目（CIP）数据

网络安全实验教程/刘建伟等编著. —北京：清华大学出版社，2007.6
（高等院校信息安全专业系列教材）
ISBN 978-7-302-15092-3

Ⅰ. 网… Ⅱ. 刘… 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(2007)第 058183 号

责任编辑：张　民　徐跃进
责任校对：时翠兰
责任印制：何　芊

出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
c-service@tup.tsinghua.edu.cn
社 总 机：010-62770175　　**邮购热线**：010-62786544
投稿咨询：010-62772015　　**客户服务**：010-62776969

印 刷 者：北京密云胶印厂
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185×230　　**印　　张**：29.75　　**字　　数**：591 千字
版　　次：2007 年 6 月第 1 版　　**印　　次**：2007 年 6 月第 1 次印刷
印　　数：1～3000
定　　价：39.50 元

高等院校信息安全专业系列教材

编审委员会

序

在社会信息化的进程中，信息已成为社会发展的重要资源，信息安全也成为21世纪国际竞争的重要战场。为了保护国家的政治利益和经济利益，各国政府都非常重视信息和网络安全，信息安全已成为一个世纪性、全球性的研究课题。

我国的信息安全事业正在蓬勃发展，国家领导高度重视，各部门通力合作、统筹规划，大大加快了我国信息安全产业发展的步伐。随着信息安全产业的快速发展，社会对信息安全人才的需求在不断增加，在高等教育领域大力推进信息安全的专业化教育，将是国家在信息安全领域掌握自主权、占领先机的重要举措。

目前，许多大学和科研院所已设立了信息安全专业或是开设了相关课程。很高兴中国计算机学会教育专业委员会和清华大学出版社在近期联合组织了一系列信息安全专业的研讨活动。他们以严谨负责的态度，认真组织全国各高校和科研院所的专家、学者，共同研讨信息安全专业的教育方法和课程体系，并在进行大量前瞻性研究工作的基础上，启动了“高等院校信息安全专业系列教材”的编写工作。这套教材将是我国信息安全专业的第一套完整、权威的教材，相信可以对全国的高等院校信息安全专业的建设起到很好的促进作用。

希望中国计算机学会教育专业委员会和清华大学出版社能够将这个研究课题一直做下去，也希望这套教材能够取得成功并不断完善，以促进各高等院校培养出更多、更好的信息安全专门人才，为我国的信息安全事业做出更大的贡献。

何德全

中国工程院院士

高等院校信息安全专业系列教材编审委员会名誉主编

出版说明

21世纪是信息时代，信息已成为社会发展的重要战略资源，社会的信息化已成为当今世界发展的潮流和核心，而信息安全在信息社会中将扮演极为重要的角色，它直接关系到国家安全、企业经营和人们的日常生活。随着信息安全产业的快速发展，国家对信息安全人才的需求量不断增加，但目前信息安全人才极度匮乏，远远不能满足金融、商业、公安、军事和政府等部门的需求。要解决供需矛盾，必须加快信息安全人才的培养，以满足社会的需求。为此，教育部继2001年批准在武汉大学开设信息安全本科专业之后，又批准了多所高等院校设立信息安全本科专业，而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。

信息安全是计算机、通信工程、数学等领域的交叉学科，对于这一新兴学科的培养模式和课程设置，各高校普遍缺乏经验，因此中国计算机学会教育专业委员会和清华大学出版社联合主办了“信息安全专业教育教学研讨会”等一系列研讨活动，并成立了“高等院校信息安全专业系列教材”编审委员会，由我国信息安全领域著名专家何德全院士担任名誉主编，著名学者肖国镇教授担任编委会主任，共同指导“高等院校信息安全专业系列教材”的编写工作。编委会本着研究先行的指导原则，认真研讨国内外高等院校信息安全专业的教学体系和课程设置，进行了大量前瞻性的研究工作，而且这种研究工作将随着我国信息安全专业的发展不断深入。经过编委会全体委员及相关专家的推荐和审定，确定了编写教材的作者，这些作者绝大多数都是既在本专业领域有深厚的学术造诣，又在教学第一线有丰富的教学经验的学者、专家。

本系列教材是我国第一套专门针对信息安全专业的教材，其特点是：

① 体系完整，结构合理，内容先进。

② 适应面广，能够满足信息安全、计算机、通信工程等相关专业对信息安全领域课程的教材要求。

③ 立体配套，除主教材外，还配有多媒体电子教案、习题与实验指导等。

④ 版本更新及时，紧跟科学技术的新发展。

为了保证出版质量，我们坚持宁缺毋滥的原则，成熟一本，出版一本，并保持不断更新，力求将我国信息安全领域教育、科研的最新成果和成熟经验反映到教材中来。在全力做好本版教材，满足学生用书的基础上，还经由专家的推荐和审定，遴选了一批国外信息安全领域优秀的教材加入到本系列教材中，以进一步满足读者对外版书的需求。热切期望广大教师和科研工作者加入我们的队伍，同时也欢迎广大读者提出宝贵意见，以便我们对本系列教材的组织、编写与出版工作不断改进，为我国信息安全专业的教材建设与人才培养做出更大的贡献。

“高等院校信息安全专业系列教材”现已正式列入普通高等教育“十一五”国家级教材规划（见教高[2006]9号文件《教育部关于印发普通高等教育“十一五”国家级教材规划选题的通知》）。我们会严把出版环节，保证规划教材的编校和印刷质量，按时完成出版任务。规划教材将进一步体现科学性、系统性和新颖性，及时反映教学改革和课程建设的新成果，并随着信息安全学科的发展及时修订。

我们的 E-mail 地址是：zhangm@tup.tsinghua.edu.cn；联系人：张民。

中国计算机学会教育专业委员会

清华大学出版社

2006 年 9 月

前言

目前，国内许多高校都设有密码学、信息安全和信息对抗专业。为了配合这些专业的理论教学工作，有的高校已建有信息安全实验室，并开设了信息安全实验课程。虽然现有的信息安全书籍很多，但是很难找到一本好的实验教材。其中一些信息安全书籍要么面向网络安全工程师的培训，要么专门介绍一些黑客攻防工具，以迎合黑客爱好者对网络攻防的兴趣和爱好，它们都不适合作为信息安全实验教材；另有一些已出版的信息安全实验教材内容并不全面，未包括无线网络安全实验和专用测试仪器的操作与使用。因此，作者萌生了编写此实验教材的念头。由于作者长期从事信息安全教学和网络安全产品的开发工作，深知读者需要了解哪些方面的知识，这无疑是写好本教材的关键。

在本书写作中，作者力求做到理论与实践相结合，课程内容与实验相结合。本实验教程选用主流的软件工具、硬件设备以及测试仪器作为实验教学工具。通过实验，让读者加深对网络安全理论知识的理解，掌握网络安全管理的技能，以期达到活学活用的目的。实践出真知——这是作者编写本书的出发点，也是广大读者所追求的目标。

本书是一本内容丰富、特色鲜明、实用性强的信息安全实验教材。该教材不仅包含了密码学常用算法的实验，而且包含了大量的网络安全工具和设备操作、计算机病毒防护等方面的内容，特别值得强调的是本书包含了主流网络安全测试仪器的操作和使用。此外，针对网络安全的发展趋势，本书安排了无线网络安全的实验内容。熟练使用这些工具、设备和仪器，对于丰富读者的网络安全实践经验，提高读者的网络安全管理水平，具有非常重要的意义。

此外，该教材在每个实验的后面均附有实验报告和思考题，便于读者对实验过程和结果进行分析和总结，并对所提出的问题进行深入思考。

全书共分 10 章。第 1 章是信息安全实验室网络环境建设实验；第 2 章是最具代表性的密码算法实验；第 3 和第 4 章是网络攻防实验；第 5～7 章是

操作系统安全实验；第 8 和第 9 章是网络安全设备和应用系统实验；第 10 章是网络安全专用测试仪器操作实验。

本书不但可以作为密码学、信息安全、信息对抗等专业的博士生、硕士生和本科生专业课程配套实验教材，而且也可以作为信息安全工程师的培训教材。

参加本书编写的人员有刘建伟、张卫东、刘培顺、李晖、魏志强等，全书由刘建伟进行了统稿和审校。本书的第 1 章和第 8 章由刘建伟编写，第 2 章由张卫东、李晖、刘建伟编写，第 3～4 章由刘建伟和刘培顺编写，第 5～7 章由刘培顺和魏志强编写，第 9 章由张卫东、李晖编写，第 10 章由刘建伟编写。此外，杨东凯和姜斌斌对第 3 章部分内容进行了补充。由于时间有限，书中难免存在不妥之处，恳请广大读者批评指正。

在本书的编写过程中，北京航空航天大学的张其善教授、西安电子科技大学的王育民教授、中国海洋大学的魏志强教授均给予作者深切的关怀与鼓励。作者要特别感谢北京航空航天大学电子信息工程学院的王祖林副院长和王力军老师，他们为北航信息安全实验室的建设提供了大力的支持和帮助。同时也感谢胡国英和李昕老师的帮助。

北航的李胜广、崔玮、郭克强、刘淳、胡荣磊、丁晓宇等博士生，池毅韬、杜大海、杨大伟、霍芝、张建荣、张晶、郑海龙、周相仲等硕士生和参加毕业设计的本科生，以及西电和海大的博士生和硕士生们为本书的顺利出版做了很多工作，作者在此一并向他们表示真诚的感谢。

最后要特别感谢上海交通大学的陈克非教授，作为本书的责任编委，陈克非教授认真审阅了全书并提出了许多宝贵的意见和建议，作者在此表示衷心的感谢。

本书得到了国家自然科学基金项目（60672102）、国家 863 计划课题（2006AA01Z422）和武器装备预研基金项目（9140A21050107HK0114）的支持。

作　者

2007 年 5 月于北京

目录

第1章 实验室网络环境建设

1.1 实验室网络环境搭建

1.1.1 实验室网络拓扑结构

信息安全实验室的硬件系统包括：

- 防火墙；
- 网络入侵检测系统(NIDS)；
- 虚拟专用网(VPN)；
- 物理隔离网卡；
- 路由器；
- 交换机；
- 集线器。

信息安全实验室的软件系统包括：

- 脆弱性扫描系统；
- 病毒防护系统；
- 身份认证系统；
- 网络攻防软件；
- 主机入侵检测软件；
- 因特网非法外联监控软件。

信息安全实验室的网络拓扑结构如图 1-1 所示。

1.1.2 实例介绍

在实验室网络拓扑结构中，一个局域网的主机 IP 地址按照图 1-2 设置，而另外两个网络中主机的 IP 地址则按照 192.168.2.11～192.168.2.20 和 192.168.3.11～192.168.3.20 来设置。注意，一个局域网中的主机数量可以根据学生分组人数的多少来设计。在本网络安全方案设计中，假设一个班有30名学生，分3组，每组10人。如果学生

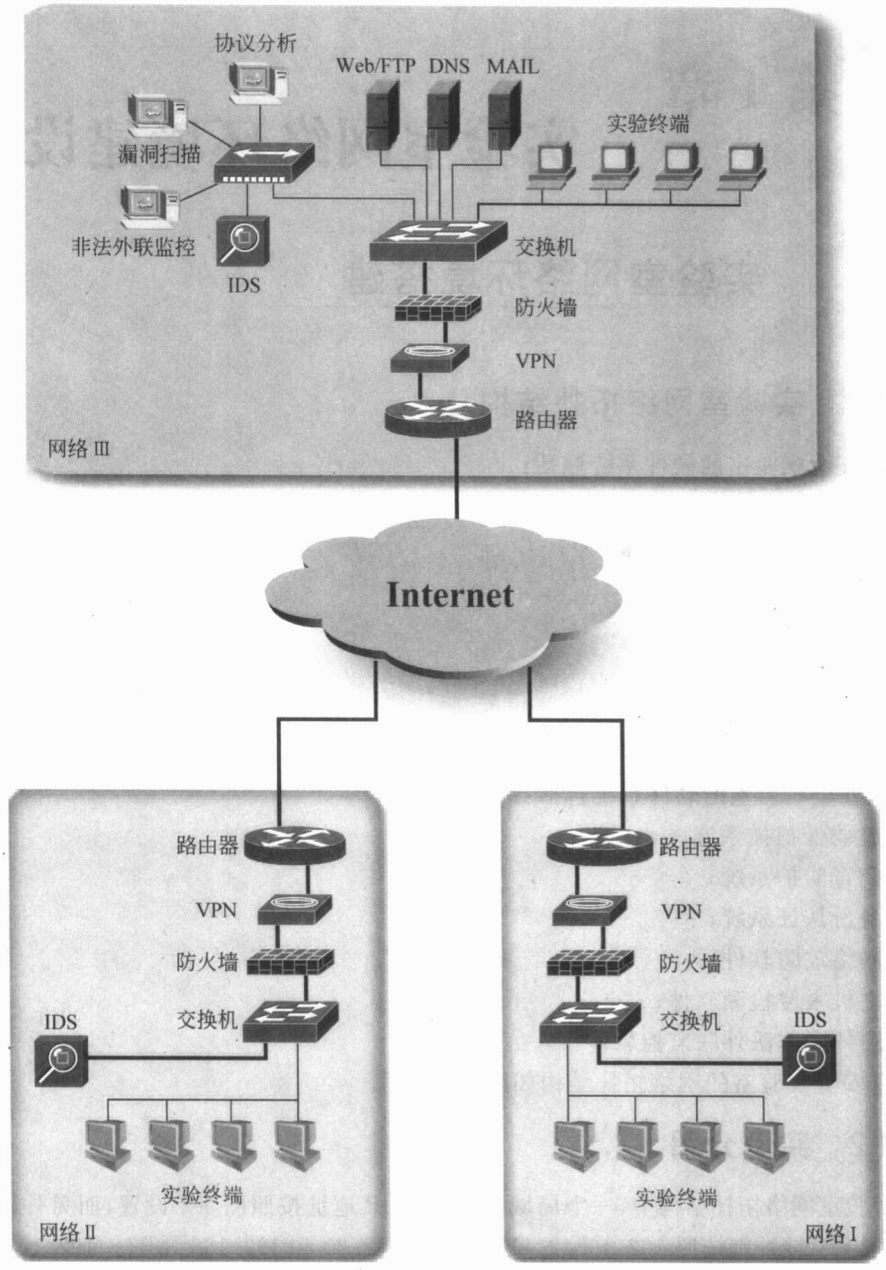

图 1-1　实验室网络拓扑结构

人数比较多，可以适当地增加每个局域网中主机的数目，或者增加局域网的个数。当然，这需要增加设备和投资。

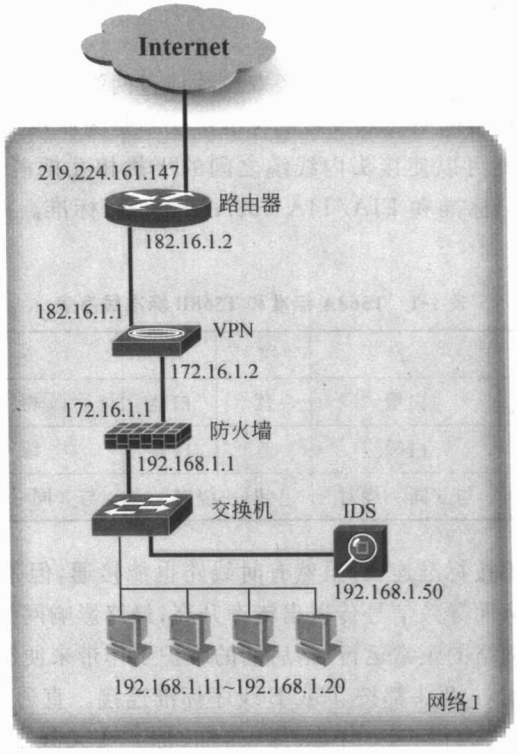

图 1-2 子网络 IP 地址设置

1.2 网络综合布线

1.2.1 网线制作

目前，局域网构建已经极为普遍，小型局域网无处不在，例如，家庭局域网、网吧、校园局域网和小型办公网等。在搭建网络的时候，网线的制作是读者需要掌握的最基本技能。网线制作的整个过程都要准确到位，排序的错误和压制的不到位都将直接影响网线的使用，出现网络不通或者网速缓慢。