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

教育部高等学校信息安全类专业教学指导委员会
中国计算机学会教育专业委员会 共同指导

顾问委员会主任：沈昌祥 编委会主任：肖国镇

计算机网络安全实验教程

曹晟 陈峥 编著

Information Security

http://www.tup.com.cn

根据教育部高等学校信息安全类专业教学指导委员会制订的《信息安全专业指导性专业规范》组织编写

清华大学出版社

“十一五”国家级规划教材

信息安全专业系列教材

教育部高等学校信息安全类专业教学指导委员会
中国计算机学会教育专业委员会 共同指导

顾问委员会主任：沈昌祥 编委会主任：肖国镇

计算机网络安全实验教程

曹晟 陈峥 编著

Information Security

http://www.tup.com.cn

根据教育部高等学校信息安全类专业教学指导委员会制订的《信息安全专业指导性专业规范》组织编写

清华大学出版社
北京

内 容 简 介

《计算机网络安全实验教程》从网络基础开始引导读者对网络的基本兴趣和认识，从网络攻防的实用性角度切入，以系统安全的全局视角对不同系统平台的网络安全案例进行练习，是编者总结信息安全专业“信息与网络安全课程”的教学经验以及实验指导的体会之集成。

本书以网络安全原理为主线，辅以其他计算机主干课程内容，突出网络安全领域知识的系统性、综合性，每个实验都与相关的计算机知识相结合，使读者建立起计算机网络安全的基本概念与完整架构。每个实验分别由实验目的、背景知识、实验步骤和思考题构成，“实验目的”明确每个实验读者需要掌握的基本知识点，通过“背景知识”的介绍让读者对实验过程背后的原因和原理有所把握，“实验步骤”结合图例详细讲解每个实验的操作方法和过程，通过设置趣味思考题使得读者对每次实验进行深化，有助于读者对实验重点的理解和拓展，这是本书的特色之一。每个实验既注重独特性的阐述，又适时解剖各实验之间的关联。

本书不仅可以作为高等院校计算机专业、网络管理专业、信息安全专业、通信专业的教材，也可以作为计算机网络安全的培训、自学教材。

图书在版编目（CIP）数据

计算机网络安全实验教程 / 曹晟，陈峥编著. --北京：清华大学出版社，2011.11
（高等院校信息安全专业系列教材）
ISBN 978-7-302-26454-5

Ⅰ. ①计… Ⅱ. ①曹… ②陈… Ⅲ. ①计算机网络－安全技术－高等学校－教材
Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2011)第 165557 号

责任编辑：张　民　赵晓宁
责任校对：白　雷
责任印制：王秀菊

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
社　总　机：010-62770175　　**邮　购**：010-62786544
投稿与读者服务：010-62795954，jsjjc@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn

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：185×260　　**印　张**：27.5　　**字　数**：654 千字
版　　次：2011 年 11 月第 1 版　　**印　次**：2011 年 11 月第 1 次印刷
印　　数：1～3000
定　　价：39.50 元

产品编号：037808-01

高等院校信息安全专业系列教材

编审委员会

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，它会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，全球对信息安全人才的需求量不断增加，但我国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，以满足社会对信息安全人才的需求。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、物理、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，确定了本丛书首批教材的作者，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，以进一步满足大家对外版书的需求。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对本系列教材提出宝贵意见，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作出更大的贡献。

“高等院校信息安全专业系列教材”已于2006年年初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。

2007年6月，教育部高等学校信息安全类专业教学指导委员会成立大会暨第一次会议在北京胜利召开。本次会议由教育部高等学校信息安全类专业教学指导委员会主任单位北京工业大学和北京电子科技学院主办，清华大学出版社协办。教育部高等学校信息安全类专业教学指导委员会的成立对我国信息安全专业的发展将起到重要的指导和推动作用。“高等院校信息安全专业系列教材”将在教育部高等学校信息安全类专业教学指导委员会的组织和指导下，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，并随着我国信息安全学科的发展不断修订和完善。

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

清华大学出版社

前言

随着信息化进程的深入和因特网的迅速发展，人们的工作、学习和生活方式正在发生着巨大变化。但必须看到，紧随信息化发展而来的网络安全问题也日渐突出。同时伴随着网络应用的日益普及和更为复杂，各种网络安全事件不断发生，计算机病毒网络化趋势越来越明显，垃圾邮件日益猖獗，黑客攻击呈指数增长，利用因特网传播有害信息手段日益翻新……网络安全问题已成为信息时代人类共同面临的挑战，国内的网络安全问题也日益突出。

各大高校需要一本良好的实验教材为导向，使同学们能更好地了解网络上各种攻击和防御技术，为以后在网络安全界的发展打下良好基础。《计算机网络安全实验教程》正是在这种环境下面世，该书为读者全面展现了各种常见网络攻防技术，使各位初学者知攻而懂防，掌握网络安全从业者所必备的基础知识。

本书从网络配置、TCP/UDP 协议等基础知识出发，之后从攻击和防御两个方面比较全面地向读者展示出当今安全界主流的攻防技术。书中既包含比较详细的主流攻击技术，同时又从防御的角度详细给出了各种攻击手段的防御技术。

本着充分发挥学生的个性和自主性，充分调动学生的学习积极性、主动性的原则，本书主要有 4 个特点：

（1）知识面宽而新

教材具有较强的综合性和技术性，可以系统地锻炼学生的实践能力，让学生在掌握基本原理的基础上学会自主实践、自主思考。在实验背景、实验步骤和思考题的设置方面不再拘泥于固有的格式模板，在保证同学们理解实验原理的基础上更多地介绍最新的技术环境，让同学们能接触相关技术的延伸介绍，为后续的延伸学习打下良好基础。

（2）可操作性强

毫无疑问，计算机技术是一门动手能力比较强的学科。本书一个很大的特点是使实验案例化。书中大量实验都是基于一个个具体的安全案例而编写，全书以“螺旋上升”的方式展现攻与防。

（3）着重同学们的思考和创新能力

该教材在每个实验之后都设置有思考题以帮助同学们学习。值得一提的是，所有思考题都以故事形式引出，激发学生的阅读兴趣，在阅读中思考，

在快乐中进步。

(4) 强调攻与防的对立统一

辩证地看,网络安全中的攻击与防御两者缺一不可,没有攻击技术,防御技术也就失去了意义,成为摆设;没有了防御技术,攻击技术就会失去发展的可能性。本书同时扮演攻击者和防御者的角色,虽然会详细模拟攻击过程,但其目的是为了在防御的时候更游刃有余。在具体介绍防御技术的同时,也会讨论如何突破防御体系,进而推出更适当的防御技术。

综上,本书是一本实用性较强的网络安全教材,内容全面,浅显易懂,实用性强。通过大量的实例和具体操作为读者展现出一个网络安全从业人员必备的各种基础知识。可作为高等学校信息安全相关专业的网络安全实验教材,也可以作为对网络安全技术感兴趣的读者参考使用。

全书共分为三大部分(7 章),主要内容如下:

第一部分为网络基础,包括两章 9 个实验。主要介绍网络的配置与连接,TCP/UDP 协议,作为本课程所需的必备基础知识。

第二部分为网络攻防,包含 3 章 16 个实验。从网络探测与扫描技术到网络攻击技术,再到网络系统安全防御技术。本部分详细地为读者展现了当今主流的网络攻击手段与相关防御技术,使读者在清楚各种攻防原理的同时也能懂得相应的实际操作。

第三部分为系统安全,包含两章 9 个实验。该部分主要讨论各种系统的安全配置以及攻击的检测与响应,使读者明白主流服务器操作系统的安全配置以及在服务器遭受入侵之后懂得如何做出应急响应。

本书由曹晟主编,其中第一和第二部分由曹晟编写,第三部分由陈峥编写,全书由曹晟统稿、定稿。在编写过程中得到了电子科技大学计算机科学与工程学院众多老师们的大力支持,在此致以深切的敬意。

限于编者的水平,书中难免有不足之处,敬请专家、同行以及广大读者批评指正。

编　者

2011 年 7 月

目 录

第一部分 网络基础

第二部分 网络攻防

第三部分 系统安全

第一部分

网络基础

第1章 网络配置与连接

1.1 网络工作站的客户端配置

1.1.1 实验目的

(1) 掌握如何配置网络工作站的客服端。

(2) 掌握如何通过命令得到IP地址配置信息、DNS地址和网关地址。

(3) 掌握如何利用Windows图形用户界面(GUI)配置网卡以使用给定的IP地址。

(4) 掌握ping、ifconfig、arp命令。

(5) 熟悉怎样测试两台计算机之间的网络连接。

1.1.2 背景知识

1. OSI的7层模型

1977年,国际标准化组织(ISO)提供了一种不基于特定机型、操作系统或公司的网络体系结构,即开放系统互连参考模型(Open System Interconnection,OSI)。OSI定义了异种机连网的标准框架,为连接分散的"开放"系统提供了基础。OSI参考模型采用分层结构化技术,将整个网络的通信功能分为7层,由低层至高层分别是物理层、数据链路层、网络层、传输层、会话层、表示层、应用层。OSI给出的仅是一个概念上和功能上的标准框架,是将异构系统互连的标准分层结构。它定义的仅是一种抽象结构,而并非是具体实现的描述,模型本身不是一组有形的可操作的协议集合,既不包括任何具体的协议定义,也不包括强制的实现一致性。网络体系结构与实现无关。

OSI模型各层的基本功能如下。

(1) 物理层。提供为建立、维护和拆除物理链路所需的机械的、电气的、功能的和规程的特性;提供有关在传输介质上传输非结构的位流及物理链路故障检测指示。机械特性规定了物理连接时接插件的规格尺寸、引脚数量和排列情况等。电气特性规定了在物理连接上传输二进制位流时线路上信号电压高低、阻抗匹配、传输速率和距离限制等。功能特性是指对各个信号线分配确切的信号含义,即定义DTE/DCE间各个线路的功能。规程特性定义了利用信号线进行二进制位流传输的一组操作规程,是指在物理连接的建立、维持、交换信息时,DTE/DCE双方在各电路上的动作序列。

(2) 数据链路层。数据链路可以粗略地理解为数据通道。物理层要为终端设备间的数据通信提供传输媒体及其连接。媒体是长期的,连接是有生存期的。在连接生存期内,