21世纪

高等学校信息安全专业规划教材

# 计算机网络安全与实验教程

马丽梅 王长广 马彦华 主编
赵冬梅 主审

清华大学出版社

21世纪高等学校信息安全专业规划教材

# 计算机网络安全与实验教程

马丽梅　王长广　马彦华　主编
赵冬梅　主审

清华大学出版社
北京

## 内 容 简 介

本书是一本网络安全方面的专业图书，由浅入深、内容详尽，图文并茂，系统而又全面地介绍了计算机网络安全技术。全书共分四部分。第一部分主要介绍计算机网络安全基础知识、网络安全的现状和评价标准以及在安全方面常用的一些网络命令；第二部分介绍了网络安全的两大体系结构的防御知识，包括操作系统的安全、密码知识、防火墙和入侵检测的内容；第三部分介绍了网络安全的两大体系结构的攻击知识，主要介绍了一些攻击的技术和方法；第四部分是实验，共包括了 34 个实验，实验和前面的理论相配套使用，通过实验更好地体会网络安全的理论知识。

本书结构清晰、易教易学、实例丰富、可操作性强，既可作为本科和高职高专院校计算机专业类的教材，也可作为各类培训班的培训教材。此外，本书也非常适于从事计算机网络安全技术研究与应用人员以及自学人员参考阅读。

本书中的授课幻灯片和实验用的工具软件都可从 http://www.tup.com.cn/网站下载。



**图书在版编目(CIP)数据**

计算机网络安全与实验教程/马丽梅，王长广，马彦华主编. --北京：清华大学出版社，2014
21 世纪高等学校信息安全专业规划教材
ISBN 978-7-302-37033-8

Ⅰ. ①计… Ⅱ. ①马… ②王… ③马… 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(2014)第 143051 号

**责任编辑**：黄　芝　薛　阳
**封面设计**：杨　兮
**责任校对**：李建庄
**责任印制**：刘海龙

**出版发行**：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn，010-62795954

**印 装 者**：北京国马印刷厂
**经　　销**：全国新华书店
**开　　本**：185mm×260mm　　**印　张**：17.25　　**字　数**：431 千字
**版　　次**：2014 年 10 月第 1 版　　**印　次**：2014 年 10 月第1 次印刷
**印　　数**：1～2000
**定　　价**：34.50 元

产品编号：057217-01

# 出版说明

由于网络应用越来越普及，信息化的社会已经呈现出越来越广阔的前景，可以肯定地说，在未来的社会中电子支付、电子银行、电子政务以及多方面的网络信息服务将深入到人类生活的方方面面。同时，随之面临的信息安全问题也日益突出，非法访问、信息窃取、甚至信息犯罪等恶意行为导致信息的严重不安全。信息安全问题已由原来的军事国防领域扩展到了整个社会，因此社会各界对信息安全人才有强烈的需求。

信息安全本科专业是2000年以来结合我国特色开设的新的本科专业，是计算机、通信、数学等领域的交叉学科，主要研究确保信息安全的科学和技术。自专业创办以来，各个高校在课程设置和教材研究上一直处于探索阶段。但各高校由于本身专业设置上来自于不同的学科，如计算机、通信和数学等，在课程设置上也没有统一的指导规范，在课程内容、深浅程度和课程衔接上，存在模糊不清、内容重叠、知识覆盖不全面等现象。因此，根据信息安全类专业知识体系所覆盖的知识点，系统地研究目前信息安全专业教学所涉及的核心技术的原理、实践及其应用，合理规划信息安全专业的核心课程，在此基础上提出适合我国信息安全专业教学和人才培养的核心课程的内容框架和知识体系，并在此基础上设计新的教学模式和教学方法，对进一步提高国内信息安全专业的教学水平和质量具有重要的意义。

为了进一步提高国内信息安全专业课程的教学水平和质量，培养适应社会经济发展需要的、兼具研究能力和工程能力的高质量专业技术人才。在教育部相关教学指导委员会专家的指导和建议下，清华大学出版社与国内多所重点大学共同对我国信息安全人才培养的课程框架和知识体系，以及实践教学内容进行了深入的研究，并在该基础上形成了“信息安全人才需求与专业知识体系、课程体系的研究”等研究报告。

本系列教材是在课程体系的研究基础上总结、完善而成，力求充分体现科学性、先进性、工程性，突出专业核心课程的教材，兼顾具有专业教学特点的相关基础课程教材，探索具有发展潜力的选修课程教材，满足高校多层次教学的需要。

本系列教材在规划过程中体现了如下一些基本组织原则和特点。

(1) 反映信息安全学科的发展和专业教育的改革，适应社会对信息安全人才的培养需求，教材内容坚持基本理论的扎实和清晰，反映基本理论和原理的综合应用，在其基础上强调工程实践环节，并及时反映教学体系的调整和教学内容的更新。

(2) 反映教学需要，促进教学发展。教材要适应多样化的教学需要，正确把握教学内容和课程体系的改革方向，在选择教材内容和编写体系时注意体现素质教育、创新能

力与实践能力的培养，为学生知识、能力、素质协调发展创造条件。

（3）实施精品战略，突出重点。规划教材建设把重点放在专业核心（基础）课程的教材建设上；特别注意选择并安排一部分原来基础比较好的优秀教材或讲义修订再版，逐步形成精品教材；提倡并鼓励编写体现工程型和应用型的专业教学内容和课程体系改革成果的教材。

（4）支持一纲多本，合理配套。专业核心课和相关基础课的教材要配套，同一门课程可以有多本具有各自内容特点的教材。处理好教材统一性与多样化，基本教材与辅助教材、教学参考书，文字教材与软件教材的关系，实现教材系列资源的配套。

（5）依靠专家，择优落实。在制定教材规划时依靠各课程专家在调查研究本课程教材建设现状的基础上提出规划选题。在落实主编人选时，要引入竞争机制，通过申报、评审确定主编。书稿完成后认真实行审稿程序，确保出书质量。

繁荣教材出版事业，提高教材质量的关键是教师。建立一支高水平的、以老带新的教材编写队伍才能保证教材的编写质量，希望有志于教材建设的教师能够加入到我们的编写队伍中来。

**21 世纪高等学校信息安全专业规划教材**

**联系人：魏江江 weijj@tup.tsinghua.edu.cn**

# 前　言

随着我国社会经济和信息技术的发展，计算机网络已经渗透到我们生活的方方面面。然而由于网络自身固有的脆弱，使网络安全存在很多潜在的威胁。在当今这样“数字经济”的时代，网络安全显得尤为重要，也受到人们越来越多的关注。网络安全技术课程已经成为计算机类及网络工程专业的必修课程，本书可作为本科院校、高等职业院校、成人教育计算机网络、通信工程等专业的教材，也可作为网络安全的培训教材。

全书分为四个部分，具体内容介绍如下：

第一部分是网络安全基础知识，包括两章：第1章为计算机网络安全概述，介绍了网络安全的定义、基本要求、网络安全的两大体系结构、网络安全的现状、立法和评价标准。第2章为网络安全协议基础，分析了IP协议、TCP协议、UDP协议和ICMP协议的结构并介绍了一些常用的网络命令。

第二部分是网络安全防御技术，包括三章：第3章为操作系统的安全配置，介绍了Linux下的安全守则和Windows Server的安全配置。第4章为密码学基础，介绍了密码学的基本概念和三种加密算法、数字签名和数字信封，数字水印技术等。第5章为防火墙与入侵检测，介绍了防火墙和入侵检测的定义，以及防火墙的分类及建立步骤，入侵检测的方法，它们的区别与联系。

第三部分是网络安全攻击技术，包括三章：第6章为黑客与攻击方法，介绍了黑客攻击的五部曲，以及相关的攻击工具与SQL注入攻击、旁注攻击、XSS攻击。第7章为DoS和DDoS，介绍了SYN风暴、Smurf攻击以及DDoS的特点。第8章为网络后门与隐身，介绍了后门的定义及实现后门和隐身的方法。

第四部分是实验，包括全部章节的34个实验。

本书在讲解相关理论的同时，附有大量的图例，尤其是第四部分实验，图片就有180多个，做到了理论知识和实际操作的紧密结合。本书是一本讲授用的教材，又是一本实用的实验指导书。

本书由马丽梅、王长广、马彦华主编，赵冬梅教授主审，参加本书编写的还有郭晴、于富强、李瑞台、侯卫红、李大顺、悦东明、井波等，本教材总计分9章，其中具体的编写任务如下：本书第1章由马丽梅编写，第2章由王长广编写，第3章由郭晴、马丽梅编写，第4章由马丽梅、于富强编写，第5章由马丽梅、李瑞台编写，第6章由马彦华编写，第7章由马丽梅编写，第8章由侯卫红编写，第9章由马丽梅、李大顺、悦东明、井波编写。全书由马丽梅统稿。

特别感谢赵冬梅教授对本书编写的悉心指导和审核，在编写过程中吸取了许多网络安全方面的专著、论文的思想，得到了许多老师的帮助，在此一并感谢。

由于作者水平有限，加上网络安全技术发展迅速，本书不足之处在所难免，敬请广大老师和专家批评指正，作者 E-mail 为 malimei@hebtu.edu.cn。

编　者

2014 年 8 月

# 目　录

## 第一部分　计算机网络安全基础

## 第二部分 网络安全的防御技术

## 第三部分　网络安全的攻击技术

## 第四部分 实 验

# 第一部分　计算机网络安全基础

# 第1章　计算机网络安全概述

- 掌握网络安全的定义、网络安全的基本要求、网络安全的两大体系：攻击和防御。
- 了解网络安全的现状、网络立法和评价标准。

随着我国社会经济的发展，计算机网络也迅速普及，渗透到我们生活的方方面面。然而由于网络自身固有的脆弱，网络安全存在很多潜在的威胁。在当今这样“数字经济”的时代，网络安全显得尤为重要，也受到人们越来越多的关注。

计算机网络安全面临的问题很多，可以分为以下三种。

**1. 自然灾害**

计算机信息系统仅仅是一个智能的机器，易受自然灾害及环境（温度、湿度、振动、冲击、污染）的影响。目前，我们不少计算机房抵御自然灾害和意外事故的能力较差，日常工作中因断电而导致设备损坏、数据丢失的现象时有发生。由于噪声和电磁辐射，网络信噪比下降，误码率增加，信息的安全性、完整性和可用性受到威胁。

**2. 黑客攻击**

这种人为的恶意攻击是计算机网络所面临的最大威胁，也是网络安全防范策略的首要对象。黑客一旦非法入侵资源共享广泛的政治、军事、经济和科学等领域，盗用、暴露和篡改大量在网络中存储和传输的数据，其造成的损失是无法估量的。

**3. 计算机病毒**

计算机病毒是一种会通过修改其他程序来把自身或其变种复制进去的程序。种类繁多的计算机病毒，如“CIH”、“情人节”、“熊猫烧香”、“蠕虫”、“木马”等病毒利用自身的“传染”能力，严重破坏数据资源，影响计算机使用功能，甚至导致计算机系统瘫痪。目前，几乎80%应用网络都受到过计算机病毒的侵害。

## 1.1　信息安全和网络安全

信息安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科，是一门交叉学科。广义上讲，信息安全涉及多方面的理论和应用知识，除了数学、通信、计算机等自然科学外，还涉及法律、心理学等社会科学，而网络安全是信息安全学科的重要组成部分。

计算机网络安全被计算机网络安全国际标准化组织（International Organization of Standards，ISO）定义为：计算机网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。网络安全包含网络设备安全、网络信息安全、网络软件安全。从广义来

说，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。

### 1.1.1 网络安全的基本要求

信息安全的目标是保护信息的保密性、机密性、完整性、可用性、可靠性、不可抵赖性和可控性，也有观点认为是机密性、完整性和可用性，即 CIA(Confidentiality, Integrity and Availability)。

**1. 机密性、保密性(Confidentiality)**

机密性是指保证信息不能被非授权访问，即使非授权用户得到信息也无法知晓信息内容，因而不能使用。保密性是指网络信息不被泄露给非授权的用户、实体或过程，即信息只为授权用户使用。保密性是在可靠性和可用性基础之上，保障网络信息安全的重要手段。常用的保密技术包括以下几项。

(1) 物理保密：利用各种物理方法，如限制、隔离、掩蔽、控制等措施，保护信息不被泄露。

(2) 防窃听：使对手接收不到有用的信息。

(3) 防辐射：防止有用信息以各种途径辐射出去。

(4) 信息加密：在密钥的控制下，用加密算法对信息进行加密处理，即使对手得到了加密后的信息也会因为没有密钥而无法读懂有效信息。

**2. 完整性(Integrity)**

完整性是网络信息未经授权不能进行改变的特性，即网络信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性。完整性是一种面向信息的安全性，它要求保持信息的原样，即信息的正确生成、正确存储和正确传输。信息的完整性包括两个方面：

① 数据完整性：数据没有被未授权篡改或者损坏。

② 系统完整性：系统未被非法操纵，按既定的目标运行。

完整性与保密性不同，保密性要求信息不被泄露给未授权的人，而完整性则要求信息不致受到各种原因的破坏。影响网络信息完整性的主要因素有：设备故障、误码(传输、处理和存储过程中产生的误码，定时的稳定度和精度降低造成的误码，各种干扰源造成的误码)、人为攻击、计算机病毒等。保障网络信息完整性的主要方法有以下几种。

(1) 协议：通过各种安全协议可以有效地检测出被复制的信息、被删除的字段、失效的字段和被修改的字段。

(2) 纠错编码方法：由此完成检错和纠错功能，最简单和常用的纠错编码方法是奇偶校验法。

(3) 密码校验和方法：它是抗篡改和防止传输失败的重要手段。

(4) 数字签名：保障信息的真实性。

(5) 公证：请求网络管理或中介机构证明信息的真实性。

**3. 可用性(Availability)**

可用性是指保障信息资源随时可提供服务的能力特性，即授权用户根据需要可以随时