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

网络攻击与防御技术

张玉清 主编

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

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

网络攻击与防御技术

张玉清 主编

Information Security

http://www.tup.com.cn

清华大学出版社
北京

内 容 简 介

本书从计算机网络安全基础知识入手，结合实际攻防案例，由浅入深地介绍网络攻击与防御的技术原理和方法。

本书共分 13 章，主要讲述网络安全的基本概念和目前黑客常用的一些攻击手段和使用技巧，包括网络扫描、口令破解技术、欺骗攻击、拒绝服务攻击、缓冲区溢出技术、Web 攻击、特洛伊木马、计算机病毒等，并针对各种攻击方法介绍对应的检测或防御技术，此外，还简要阐述了目前应用较为广泛的多种典型防御手段，包括加密、身份认证、防火墙、入侵检测系统、虚拟专用网、蜜罐取证等。

本书内容全面，讲解细致，可作为高等院校信息安全等相关专业教学用书，也可供计算机网络的系统管理人员、安全技术人员和网络攻防技术爱好者学习参考之用。

图书在版编目（CIP）数据

网络攻击与防御技术 / 张玉清主编. —北京：清华大学出版社，2011.1
（高等院校信息安全专业系列教材）
ISBN 978-7-302-23400-5

Ⅰ. ①网… Ⅱ. ①张… 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（2010）第 153315 号

责任编辑：张　民　李玮琪
责任校对：梁　毅
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
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**：21.25　**字　数**：498 千字
版　　次：2011 年 1 月第 1 版　　**印　次**：2011 年 1 月第1 次印刷
印　　数：1～4000
定　　价：33.00 元

产品编号：039704-01

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做出更大的贡献。

“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地址是：zhangm@tup.tsinghua.edu.cn；联系人：张民。

清华大学出版社

前言

计算机和信息技术的飞速发展，网络的日益普及，深刻地改变着人们的生活方式、生产方式与管理方式，加快了国家现代化和社会文明的发展。21世纪的竞争是经济全球化和信息化的竞争，“谁掌握信息，谁就掌握了世界”，信息安全不仅关系到公民个人、企业团体的日常生活，更是影响国家安全、社会稳定至关重要的因素之一。

近年来，我国网络安全事件发生比例呈上升趋势，调查结果显示绝大多数网民的主机曾经感染病毒，超过一半的网民经历过账号/个人信息被盗窃、被篡改，部分网民曾被仿冒网站欺骗。在经济利益的驱使下，制造、贩卖病毒木马、进行网络盗窃或诈骗、教授网络攻击技术等形式的网络犯罪活动明显增多，造成了巨大的经济损失和安全威胁，严重影响了我国互联网事业的健康发展。

面对如此严峻的挑战，国家明确提出要大力加强信息安全专门人才的培养，以满足社会对信息安全专门人才日益增长的需求，目前大多数高等院校都陆续开设了信息安全方面的课程，信息安全专门人才的培养逐渐步入正轨。

本书的目的是帮助安全人员掌握网络信息安全的基本知识，了解网络攻击方法和步骤，掌握基本的网络攻防技术，树立良好的网络安全防范意识。书中总结了目前网络攻击的现状与发展趋势，详细介绍了计算机及网络系统面临的各种威胁和攻击手段。作者以实例映衬原理，理论联系实际，采用尽可能简单和直观的方式向读者讲解技术原理，演绎攻击过程，希望能通过本书，向读者揭开“黑客”的神秘面纱，使读者对网络攻防技术有进一步的了解。

本书共分为13章，内容由浅入深。第1章主要介绍了网络安全相关的基础知识和概念，阐述目前的网络安全形势，使读者对这一领域有一个初步的认识。第2章介绍了网络攻击的一般步骤。第3章至第11章则分门别类地阐述了目前黑客常用的一些攻击手段和技术，包括网络扫描技术、口令破解技术、欺骗攻击、拒绝服务攻击、缓冲区溢出、Web攻击、木马及计算机病毒等，对每种攻击手段既分析其技术原理、实现过程、性能、优缺点，又运用实际案例对知识要点进行阐释；并介绍了针对该种攻击手段可以采取的防范措施和策略。第12章介绍了目前广泛应用的多种典型防御手段，包括常用的加密技术、身份认证技术、防火墙技术、入侵检测技术、虚拟专用网

技术、日志审计技术、蜜罐取证等，从系统防御体系的角度阐述信息安全知识，加深读者对整个信息安全领域的了解和认识。第 13 章对网络安全未来的发展进行了展望，并考虑到信息安全与人文和社会科学领域的交叉交融，介绍了与网络安全相关的一些法律法规问题，强调法律在信息安全领域的重要性。

本书还备有配套的实验教程《网络攻击与防御技术实验教程》，对每个技术专题，都制定了详细的实战方案，两书结合，可以使读者在掌握攻击原理的同时，也能亲自动手，体会攻防的实战性，从而更深刻地理解网络攻防原理与技术。

本书可作为信息安全、计算机专业类本科生、硕士研究生的教科书，也适合网络管理人员、安全维护人员及相关技术人员和网络攻防爱好者参考阅读。选读本书的读者应具备基本的操作系统和计算机网络知识、以及 C/C++ 编程语言的预备知识。

本书是作者在教学和科研实践的基础上编写的，参与本书写作的有姚力、陈深龙、郎良、戴祖锋、谢崇斌、王磊和马欣等，全书由张玉清统稿。在编写过程中，对基本概念、基本知识的介绍力争做到简明扼要，各章自成体系，又相互呼应。

由于编写时间仓促，编者水平有限，书中难免出现疏漏和不当之处，加之网络攻防技术纵深宽广，发展迅速，在内容取舍和编排上，也难免考虑不周全，诚请读者批评指正。来信请给 zhangyq@nipc.org.cn，谢谢！

编者

2010 年 12 月

目录

第1章 网络安全概述

随着计算机网络技术在各领域的普遍应用，现代社会的人们对于信息网络的依赖性正与日俱增。网络的用户涵盖了社会的方方面面，大量在网络中存储和传输的数据承载着社会的虚拟财富，这对计算机网络的安全性提出了严格的要求。然而与此同时，黑客技术也在不断发展，大量黑客工具在网络上广泛流传，使用这些工具的技术门槛越来越低，从而造成全球范围内网络攻击行为的泛滥，对信息财富造成了极大的威胁。因此，掌握网络安全的知识，保护网络的安全已经成为确保现代社会稳步发展的必要条件。

本章首先从网络安全的基础知识出发，介绍了网络安全的定义和特征；接着总结了威胁网络安全的主要因素，并给出抵御这些威胁的防范措施；最后，介绍了制定安全策略的一般性原则，并对网络安全体系的设计进行了讨论。

1.1 网络安全基础知识

1.1.1 网络安全的定义

“安全”一词在字典中被定义为“远离危险的状态或特性”和“为防范间谍活动或蓄意破坏、犯罪、攻击或逃跑而采取的措施。”

网络安全从其本质上来讲就是网络上的信息安全。它涉及的领域相当广泛。从广义上来说，凡是涉及网络上的保密性、完整性、可用性、真实性和可控性的相关技术和理论，都是网络安全所要研究的领域。

网络安全的一个通用定义是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的原因而遭到破坏、更改或泄露，系统连续、可靠、正常地运行，服务不中断。

从用户（个人、企业等）的角度来说，他们希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护，避免其他人或对手利用窃听、冒充、篡改和抵赖等手段对用户的利益和隐私造成损害和侵犯，同时也希望当用户的信息保存在某个计算机系统上时，不受其他非法用户的非授权访问和破坏。

从网络运行和管理者的角度来说，他们希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现病毒、非法存取、拒绝服务和网络资源的非法占用及非法控制等威胁，制止和防御网络“黑客”的攻击。

对安全保密部门来说，他们希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免其通过网络泄露，避免由于这类信息的泄密对社会产生危害，对国家造成

巨大的经济损失，甚至威胁到国家安全。

从社会教育和意识形态角度来讲，网络上不健康的内容，会对社会的稳定和发展造成阻碍，必须对其进行控制。

因此，网络安全在不同的环境和应用中会得到不同的解释。

① 运行系统安全，即保证信息处理和传输系统的安全。包括计算机系统机房环境的保护，法律、政策的保护，计算机结构设计上的安全性考虑，硬件系统的可靠安全运行，计算机操作系统和应用软件的安全，数据库系统的安全，电磁信息泄露的防护等。它侧重于保证系统正常的运行，避免因为系统的崩溃和损坏而对系统存储、处理和传输的信息造成破坏和损失，避免由于电磁泄露产生信息泄露，干扰他人（或受他人干扰），本质上是保护系统的合法操作和正常运行。

② 网络上系统信息的安全。包括用户口令鉴别、用户存取权限控制、数据存取权限、方式控制、安全审计、安全问题跟踪、计算机病毒防治和数据加密等。

③ 网络上信息传播的安全，即信息传播后的安全，包括信息过滤等。它侧重于保护信息的保密性、真实性和完整性。避免攻击者利用系统的安全漏洞进行窃听、冒充和诈骗等有损于合法用户的行为。本质上是保护用户的利益和隐私。

显而易见，网络安全与其所保护的信息对象有关。其本质是在信息的安全期内保证其在网络上流动时或者静态存放时不被非授权用户非法访问，但授权用户却可以访问。网络安全、信息安全和系统安全的研究领域是相互交叉和紧密相连的。

本书中所讲的网络安全是指通过各种计算机、网络、密码技术和信息安全技术，保证在公有通信网络中传输、交换和存储信息的机密性、完整性和真实性，并对信息的传播及内容具有控制能力，不涉及网络可靠性、信息的可控性、可用性和互操作性等领域。

1.1.2 网络安全的特征

网络安全应具有以下 4 个方面的特征：

1）保密性

保密性指信息不泄露给非授权用户、实体、过程或供其利用的特性。

2）完整性

完整性指数据未经授权不能进行改变的特性。即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。

3）可用性

可用性指可被授权实体访问并按需求使用的特性。即当需要时应能存取所需的信息。网络环境下拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击。

4）可控性

可控性指对信息的传播及内容具有控制能力。

1.1.3 网络安全的重要性

随着网络的快速普及，网络以其开放、共享的特性对社会的影响也越来越大，信息网络已经成为社会发展的重要保证。信息网络涉及到国家的政治、军事、文教等诸多领

域，其中存储、传输和处理的信息有许多是政府文件、商业经济信息、银行资金转账、股票证券、能源资源数据、科研数据等重要信息，还有很多是敏感信息，甚至是国家机密。所以难免会吸引来自世界各地的各种人为攻击（例如信息泄露、信息窃取、数据篡改、计算机病毒等）。同时，网络实体还要经受诸如水灾、火灾、地震、电磁辐射等方面的考验。

近年来，计算机犯罪案件也急剧上升，计算机犯罪已经成为普遍的国际性问题。据美国联邦调查局的报告，计算机犯罪是商业犯罪中所占比例最大的犯罪类型之一。计算机犯罪大都具有瞬时性、广域性、专业性、时空分离性等特点。通常很难留下犯罪证据，这大大刺激了计算机高技术犯罪案件的发生。计算机犯罪率的迅速增加，使各国的计算机系统特别是网络系统面临着很大的威胁，并成为严重的社会问题之一。大量事实表明，确保网络安全已经是一件刻不容缓的大事。有人估计，未来计算机网络安全问题比核威胁还要严重，因此，研究网络安全课题具有十分重要的理论意义和实际背景。

据美国 AB 联合会组织的调查和专家估计，美国每年因计算机犯罪所造成的经济损失高达 150 亿美元。近几年国内外很多著名站点被黑客恶意修改，在社会上造成许多不良的影响，也给这些站点的运维者带来了巨大的经济损失。

利用计算机通过 Internet 窃取军事机密的事例，在国外也是屡见不鲜。美国、德国、英国、法国和韩国等国的黑客曾利用 Internet 网分别进入五角大楼、航天局、北约总部和欧洲核研究中心的计算机数据库。

我国信息化进程虽然刚刚起步，但是发展迅速，同时安全问题也日益严重。在短短的几年里，发生了多起危害计算机网络的安全事件，必须采取有力的措施来保护计算机网络的安全。广义上的网络安全还应该包括如何保护内部网络的信息不从内部泄露、如何抵制文化侵略、如何防止不良信息的泛滥等。

未来的战争将是信息战争，信息安全关系到国家的主权和利益，关系着国家的安全。因此网络安全技术研究的重要性和必要性是显而易见的。

1.2　网络安全的主要威胁因素

计算机网络的发展，使信息的共享应用日益广泛与深入。但是信息在公共通信网络上存储、共享和传输，可能面临的威胁包括被非法窃听、截取、篡改或毁坏等，这些威胁可能给网络用户带来不可估量的损失，使其丧失对网络的信心。尤其是对银行系统、商业系统、管理部门、政府或军事领域而言，信息在公共通信网络中的存储与传输过程中的数据安全问题更是备受关注。

威胁是指任何可能对网络造成潜在破坏的人、对象或事件。互联网面临的安全威胁有其他很多因素，可能是故意的，也有可能是无意的；可能来自企业外部，也有可能是内部人员造成的；可能是人为的，也有可能是自然力造成的。总结起来，大致有下面几种主要威胁。

① 非人为的、自然力造成的数据丢失、设备失效、线路阻断。