21世纪 高等学校信息安全专业规划教材

网络安全教程及实践

吴辰文 李启南 郭晓然 编著

清华大学出版社

内 容 简 介

本书系统全面地介绍了网络安全的基本概念、网络安全体系结构及网络信息安全的评价标准，在对计算机网络体系结构及协议进行简要介绍的基础上，对网络攻击和防御的理论和方法进行了较为详细、系统的介绍，对 Windows 和 Linux 操作系统平台的安全性设计和实现进行了分析。对信息加密理论与技术进行了介绍，给出了常用的网络安全设备防火墙、入侵检测/防御系统、蜜罐/蜜网的工作原理和应用领域。书中还给出了网络攻防的几个典型案例，介绍了网络安全的规划、设计和评估方法。

本书结构严谨、层次分明、概念清晰、叙述准确、实践性强，易于学习和理解，可作为高等院校计算机专业、电子信息以及通信专业高年级本科生和低年级硕士研究生教材，也可供网络安全管理人员以及开发人员作为技术参考书或工具书使用。

图书在版编目(CIP)数据

网络安全教程及实践/吴辰文等编著. --北京：清华大学出版社，2012.9
21 世纪高等学校信息安全专业规划教材
ISBN 978-7-302-28725-4

Ⅰ. ①网…　Ⅱ. ①吴…　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(2012)第 088736 号

责任编辑：郑寅堃　薛　阳
封面设计：杨　兮
责任校对：时翠兰
责任印制：何　芊

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 刷 者：北京富博印刷有限公司
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：185mm×260mm　　**印　张**：25.5　　**字　数**：618 千字
版　　次：2012 年 9 月第 1 版　　**印　次**：2012 年 9 月第1 次印刷
印　　数：1～3000
定　　价：44.50 元

产品编号：045908-01

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

网络安全主要是指保护网络信息系统使其没有危险、不受威胁、不出事故。从技术角度来说，网络安全涵盖面非常广，不仅包含威胁网络安全的各种计算机病毒、木马、恶意软件和各种方式的网络攻击行为，还有针对这些威胁的各种安全技术、设备、软件和应用配置方法以及加密、解密技术等。总之，网络安全主要涉及信息系统的保密性、完整性、真实性、可靠性、可用性和不可抵赖性等。

本书在编写的过程中，主要依据网络安全的目标，结合作者十多年来在各类企事业单位网络安全设计、规划及技术实现方面的工作经验，综合作者在网络安全课程多年进行研究生和本科生教学的经验，既考虑到对基础理论和知识的讲解，又考虑到实际应用的需要，本着易学、易掌握的原则，由浅入深、循序渐进地介绍了网络安全相关技术知识和操作方法，注重学习者理论水平和操作技能的同步提高，既具有专业性，又不乏实用性，能够很好地满足网络安全方面的教学需要。

本书共分为 13 章。第 1 章介绍了网络通信安全的基本概念和评价标准；第 2 章介绍了计算机网络的基础知识；第 3 章介绍了网络安全的基础知识；第 4～6 章介绍了网络攻击和防御技术；第 7 章和第 8 章介绍了常见的加密解密技术、防火墙和入侵检测技术；第 9～11 章介绍了基于 Linux 和 Windows 系统的安装、配置特别是安全设置；第 12 章介绍了 Web 安全和 IP 安全；第 13 章介绍了网络安全规划、设计和评估方法。

参加本书编写工作的主要有：兰州交通大学的李启南编写了第 7、第 9～12 章，西北民族大学的郭晓然编写了第 3～6 章和第 8 章，其余章节由兰州交通大学的吴辰文编写，并进行了统稿。

本书在编写过程中还得到了许多师生的帮助，特别是兰州交通大学计算机科学与技术系的硕士研究生于芳、董晓静、王平、王维、闫毅郎、吴立鹏、李贝、张耀方、石佳玉和孔德弟，为本书的编写进行了辛勤的工作，包括录入文字、绘制图表、实验平台的搭建和编程实现等，在此表示诚挚的谢意。

由于网络安全技术发展非常迅速，涉及的知识面广，加之作者水平有限，书中难免存在疏漏与不妥之处，恳请读者批评指正。对于本书中存在的不妥之处，也请有关专家和读者提出宝贵意见。

编　者

2012 年 4 月

目　录

第1章　网络安全概论

本章学习要求：

- 掌握网络安全的基本要求，了解网络安全技术的发展状况和发展趋势。
- 了解网络安全的攻防体系和层次体系结构。
- 熟悉网络通信系统面临的安全威胁。
- 了解网络安全在信息化中的重要性。
- 熟悉网络安全的目标，掌握网络安全的评价标准。

1.1　网络安全概述

1.1.1　网络安全的概念

随着信息化进程的深入和 Internet 的迅速普及，人们的工作、学习和生活方式发生了巨大变化，工作效率大幅度提高，信息资源得到最大程度的共享。但随之而来的是网络上的安全问题越来越突出，网络信息系统遭受病毒侵害乃至黑客攻击的现象越来越多，因此，保证网络信息系统的安全成为网络发展中的重要问题。据中国互联网络信息中心(CNNIC)发布的《第 24 次中国互联网络发展状况统计报告》显示，在我国，仅 2011 年上半年就有超过 2.17 亿的网民上网时遇到过病毒和木马的攻击，其中约 1.21 亿网民遇到过账号或密码被盗的问题。因此，网络安全已经成为当前各界十分关注的问题，网络钓鱼、病毒、木马等网络安全隐患的存在给网络信息技术的发展带来了极大的威胁，而在我国的网络规模和应用取得快速发展的基础上，网络应用已经从生活娱乐逐步向社会经济领域渗透，网民对网络信任和安全的要求也日渐提高。我国互联网下一步发展的重点是由可用互联网向可信互联网阶段发展，如何提高网民对互联网的信任程度，已经成为当前迫切需要解决的问题，而在“可用”的基础之上，构建“可信”的网络环境则是未来的必然趋势。因此，网络信息安全技术成为建设“可信”网络环境的重要技术手段。

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到破坏、更改、泄漏，系统连续可靠正常地运行，网络能够提供不中断服务。

网络安全从其本质上来讲就是网络上的信息安全。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。

网络安全的具体含义会随着“角度”的变化而变化。比如：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、抵赖等手段侵犯用户的利益和隐私。

从网络运行和管理者的角度，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“陷门”、病毒、非法存取、拒绝服务和网络资源非法占用和非法控制等威胁，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，避免机要信息泄漏，防止对社会产生危害、对国家造成巨大损失。

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

1.1.2 网络安全的攻防体系

网络安全的安全威胁来自于黑客的攻击，而要保证网络安全，则需要针对网络安全进行有效的防御，因此，网络安全从大的方面可以分为攻击技术和防御技术两大类。这两类技术是相辅相成互相促进而发展的。一方面，黑客进行攻击的时候，需要了解各种防御技术和方法，以便能绕过防御而对目标进行攻击；另一方面，在进行防御的时候则必须了解黑客攻击的方式方法，这样才能有效地应对各种攻击。攻击和防御永远是一对矛盾。图 1-1 则用图示的方法说明了网络安全攻防体系所涉及的内容。

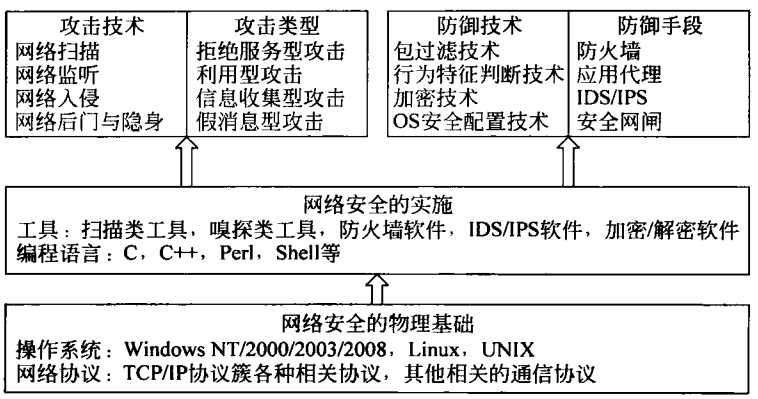

图 1-1 网络安全的攻防体系结构

攻击技术可以分为 4 大类，具体如下。

第一类是服务拒绝类攻击，包括死亡之 ping(ping of death)、泪滴(Teardrop)、UDP 洪水(UDP flood)、SYN 洪水(SYN flood)、Land 攻击、Smurf 攻击、Fraggle 攻击、电子邮件炸弹和畸形消息攻击等。

第二类是利用型攻击，包括口令猜测、特洛伊木马、缓冲区溢出。

第三类是信息收集型攻击，包括地址扫描、端口扫描、反向映射、慢速扫描、体系结构探测、DNS 域转换、Finger 服务、LDAP 服务等。

第四类是假消息攻击，主要包括 DNS 高速缓存污染、伪造电子邮件。

网络系统的防御技术主要包括以下几种技术。

(1) 包过滤技术。也是防火墙最基本的技术。包过滤技术是用来控制内、外网络数据流入和流出，通过对数据流的每个包进行检查，根据数据报的源地址、目的地址、TCP 和 UDP 的端口号，以及 TCP 的其他状态来确定是否允许数据包通过。

(2) 行为特征判断技术。属于比包过滤技术更可靠更精确的攻击判断技术，通过对攻击者一系列攻击数据包行为规律的分析、归纳、总结，并结合专家的经验，提炼出攻击识别规则知识库；模拟专家发现新攻击的机理，通过分布在用户计算机系统上的各种探针，动态监

视程序运行的动作，并将程序的一系列操作通过逻辑关系分析组成有意义的行为，再结合应用攻击识别规则知识，实现对攻击的自动识别。

(3) 加密技术。是最常用的安全保密手段，利用技术手段(加密算法)把重要的数据变为乱码(加密)传送，到达目的地后再用相同或不同的手段还原(解密)为原文。

(4) OS 安全配置技术。通过采用安全的操作系统，并对操作系统进行各种安全配置，以保证合法访问者能够进行操作和访问，隔离和阻断非法访问者的请求。

应用以上技术所采用的防御手段(或设备)通常有以下几种。

(1) 防火墙。一个由软件、硬件或者是二者结合组合而成、在内部网和外部网之间、专用网与公共网之间的界面上放置的安全设备，通过监测、限制、更改跨越防火墙的数据流，尽可能地对外部屏蔽网络内部的信息、结构和运行状况，以此来实现对网络的安全保护。

(2) 应用代理。是彻底隔断通信两端的直接通信的网络安全设备，安装了应用代理后，所有通信都必须经应用层代理转发，访问者任何时候都不能与服务器建立直接的连接，应用层的协议会话过程必须符合代理的安全策略要求，而将不符合安全要求的各种连接阻断或屏蔽，保护网络的安全。

(3) IDS/IPS(入侵检测系统/入侵防御系统)。依照一定的安全策略，对网络、系统的运行状况进行监视，尽可能发现各种攻击企图、攻击行为或者攻击结果，以保证网络系统资源的机密性、完整性和可用性。

(4) 安全网闸。是使用带有多种控制功能的固态开关读写介质连接两个独立主机系统的信息安全设备。物理隔离网闸所连接的两个独立主机系统之间，不存在通信的物理连接、逻辑连接、信息传输命令、信息传输协议，不存在依据协议的信息包转发，只有数据文件的无协议“摆渡”，且对固态存储介质只有“读”和“写”两个命令。所以，物理隔离网闸从物理上隔离、阻断了具有潜在攻击可能的一切连接，使“黑客”无法入侵、无法攻击、无法破坏，提高了受保护网络的安全性。

上面所列的技术是网络安全攻击防御体系中经常用到的技术，除了上述所列的技术以外，网络安全管理技术、身份认证与访问控制技术、病毒及恶意软件防护技术、Web 站点安全技术、数据库系统安全技术以及电子商务安全技术等也是网络安全技术所涉及的内容。

网络安全的实施过程中需要各种类型的工具，包括扫描类工具、嗅探类工具、防火墙软件、IDS/IPS 软件、加密/解密软件等。而编写这些工具采用的编程语言主要有 C、C++、Perl、Shell 等。

对于任何系统，网络的安全是根本，因此网络安全的物理基础也是网络安全的根本，网络安全的物理基础包括安全的操作系统，如 Windows NT/2000/2003/2008、Linux、UNIX 等；也包括各种网络协议，通常使用的是 TCP/IP 协议簇各种相关协议和其他相关的通信协议。

1.1.3　网络安全的层次体系

从层次体系上，可以将网络安全划分为物理层安全、系统层安全、网络层安全、应用层安全和安全管理 5 个层次，各个层次的安全性问题主要如下。

1. 物理环境的安全性(物理层安全)

网络环境的安全包括通信线路的安全、物理设备的安全、机房的安全等。该层次的安全