21世纪 高等学校信息安全专业规划教材

网络攻击与防御技术

林英 张雁 康雁 编著

清华大学出版社

21世纪高等学校信息安全专业规划教材

网络攻击与防御技术

林 英 张 雁 康 雁 编著

清华大学出版社
北京

内 容 简 介

本书主要从三个方面进行介绍，首先通过介绍一些主要的网络攻击手段，让人们了解常见网络攻击的原理和惯用手法，达到知己知彼的目的；其次通过介绍一些典型的网络安全防范技术，达到保护网络安全的目的；最后通过介绍如何利用计算机相关技术和工具查找、收集和分析处理计算机数字证据，达到网络安全侦查的目的。本书概念明确，层次清晰，注重理论联系实际，通过在每章中配有相应技术实践的例子，便于理解书中的理论知识。

本书适用于计算机、通信、信息安全专业本科高年级学生，也适合广大对网络安全侦查和防范技术感兴趣的读者阅读。

图书在版编目(CIP)数据

网络攻击与防御技术/林英，张雁，康雁编著. —北京：清华大学出版社，2015
21世纪高等学校信息安全专业规划教材
ISBN 978-7-302-38046-7

Ⅰ. ①网…　Ⅱ. ①林…　②张…　③康…　Ⅲ. ①计算机网络—安全技术　Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2014)第219360号

责任编辑：魏江江　薛　阳
封面设计：杨　兮
责任校对：梁　毅
责任印制：杨　艳

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：17.25　　字　　数：434千字
版　　次：2015年1月第1版　　印　　次：2015年1月第1次印刷
印　　数：1～2000
定　　价：34.50元

产品编号：054638-01

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

随着计算机技术和网络通信技术的飞速发展，Internet 的规模正在不断增长。Internet 的迅猛发展不仅带动了信息产业和国民经济的快速增长，也为企业的发展带来了勃勃生机，但随着计算机网络的广泛应用，与 Internet 有关的安全事件也越来越多，安全问题日益突出，各种计算机犯罪层出不穷，越来越多的组织开始利用 Internet 处理和传输敏感数据，Internet 上也到处传播和蔓延入侵方法与脚本程序，使得连入 Internet 的任何系统都处于将被攻击的风险之中。因此如何保障网络与信息资源的安全就一直是人们关注的焦点，如何对各种网络攻击手段进行检测和预防，是计算机安全中的重中之重。

面对严峻的网络安全形势，了解和掌握网络攻防知识具有重要的现实意义。一方面，研究网络攻击，是因为网络安全防范不仅要从正面去进行防御，还要从反面入手，从攻击者的角度设计更坚固的安全保障系统。另一方面，攻击方法的不断演进，防范措施也必须与时俱进。目前，很多网络安全技术的理论研究有待进一步加强，有很多值得研究的课题，随着网络安全新技术的出现，有助于加强传统安全技术的防御功能，提升网络安全的等级。本书在编写过程中注意保持教学内容的系统性，以攻和防为主线，加入了传统安全技术的最新发展动态，力求能反映网络攻防的最新发展成果。

本书共分 10 章。第 1 章为“网络安全概述”，阐述了网络安全、网络安全威胁、网络攻击及攻击防御的相关概念。第 2 章为“网络攻击的一般过程”，从攻击者的角度，将攻击过程归纳为三个阶段，并详细分析了网络攻击在不同阶段中所采用的不同攻击技术。第 3 章为“网络攻击关键技术原理剖析”，主要针对目前常见的网络攻击手段（如口令破解、网络嗅探、网络扫描、网络欺骗、缓冲区溢出攻击、拒绝服务攻击）进行介绍并给出相应的防御方法。第 4 章为“计算机病毒原理及防治”，介绍了计算机病毒的原理、木马技术、反病毒技术的原理并介绍了如何查杀恶意程序。第 5 章为“防火墙技术”，介绍防火墙的相关技术及最新发展动态。第 6 章为“入侵检测技术”，介绍入侵检测的相关技术，总结了入侵检测的主要研究方向。第 7 章为“漏洞挖掘技术”，主要阐述安全漏洞现状及漏洞挖掘的相关技术。第 8 章为“网络诱骗技术”，介绍常见网络诱骗的相关技术及工具。第 9 章为“计算机取证”，介绍如何利用计算机相关技术和工具查找、收集和分析处理计算机数字证据。第 10 章为“应急响应、备份和恢复”，从响应、备份和恢复的角度介绍了如何提高应急响应能力。为了使读者能检查学习效果，每章都附有习题及相关实验内容。

在本书编写过程中，作者主要总结了多年网络攻防本科教学的内容及参考了近年

来的文献资料。在写作中，作者力求做到层次清楚，语言简洁流畅，内容丰富，既便于读者循序渐进地系统学习，又能使读者了解到网络攻防技术新的发展，希望本书对读者掌握网络攻防有一定的帮助。

本书的第2、3、4、9章由林英执笔完成，第5、6、7、8章由张雁执笔完成，第1、10章由康雁执笔完成，全书由林英统稿，书中的实验大部分由杜磊同学完成。本书的完成，得到了云南大学软件学院教材建设项目及云南省省级特色专业“信息安全专业”建设的资助，在此谨表衷心的感谢。

限于学术水平，错误与不妥之处在所难免，敬请读者批评指正，编者将不胜感激。

编者

2014年10月

目　录

第1章　网络安全概述

本章学习目标：

- 了解网络安全；
- 掌握网络安全的层次体系；
- 了解网络安全威胁及常见的网络攻击；
- 了解网络攻击的防御方法；
- 了解网络与信息安全的相关标准。

1.1　网络安全简介

在 Internet 规模不断增长的同时，与 Internet 有关的安全事件也越来越多，安全问题日益突出。越来越多的组织开始利用 Internet 处理和传输敏感数据，同时在 Internet 上也到处传播和蔓延着入侵方法和脚本程序，使得连入 Internet 的任何系统都处于将被攻击的风险之中。理论分析表明，诸如计算机病毒、恶意代码、网络入侵等攻击行为之所以能够对计算机系统产生巨大的威胁，其主要原因在于计算机及软件系统在设计、开发、维护过程中存在安全弱点，而这些安全弱点的大量存在也是安全问题的总体形势趋于严峻的主要原因之一。

网络安全涉及的内容既有技术方面的问题，也有管理方面的问题，两方面相互补充，缺一不可。面对越来越严峻及无所不在的网络攻击，如何更有效地保护重要的信息数据、提高计算机网络系统的安全性已经成为所有计算机网络应用必须要考虑和解决的一个重要问题。

1.1.1　网络安全

1. 网络安全的定义

网络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、数论和信息论等多种学科的综合性学科，从本质上来讲网络安全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。

下面给出网络安全的一个具体定义：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，不因无意或恶意威胁而遭到破坏、更改、泄露，从而保证网络系统连续、可靠、正常地运行，网络服务不中断。对于用户而言，主要是保障个人数据或企业信息的完整、可用和保密。

随着“角度”的不同，网络安全的具体含义会有所变化。对用户（个人、企业等）而言，网络安全是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，进行隐私访问和破坏；对网络运行和管理者而言，网络资源安全主要是指有访问控制措施，无“黑客”和病毒攻击；从安全保密部门的角度来看，是指防止有害信息出现和敏感信息泄露。

具体地说，网络安全具有以下几个方面的特征。

(1) 机密性：利用密码技术对数据进行加密，保证网络中的信息不被非授权实体获取与使用。

(2) 完整性：保护计算机系统软件(程序)和数据不被非法删改，保证授权用户得到的信息是真实的。

(3) 可用性：无论何时，只要用户需要，系统和网络资源就必须是可用的，尤其是当计算机及网络系统遭到非法攻击时，它仍然能够为用户提供正常的系统功能或服务。

(4) 可控性：指授权机构对信息的内容及传播具有控制能力的特性。

(5) 可靠性：在规定的条件下和规定的时间内，完成规定功能的概率。

除此之外，不可否认性、可审查性等也被认为是网络安全应该具有的特征。

2. 网络安全的目标

网络安全的目标是确保网络系统的信息安全。网络信息安全主要包括两个方面：信息存储安全和信息传输安全。信息存储安全是指信息在静态存放状态下的安全，如是否被非授权调用等，一般通过设置访问权限、身份识别、局部隔离等措施来保证。信息传输安全是指信息在动态传输过程中的安全。

为确保网络信息的传输安全，尤其需要防止以下问题。

(1) 截获：对网上传输的信息，攻击者只需在网络的传输链路上通过物理或逻辑的手段，就能对数据进行非法的截获，进而得到用户或服务方的敏感信息。

(2) 伪造：对用户身份仿冒这一常见的网络攻击方式，传统的对策一般是采用身份认证，但是，用于用户身份认证的密码在登录时常常是以明文的方式在网络上进行传输的，很容易被攻击者在网络上截获，进而可以对用户的身份进行仿冒，使身份认证机制被攻破。

(3) 篡改：攻击者有可能对网络上的信息进行截获并且篡改其内容，使用户无法获得准确、有用的信息或落入攻击者的陷阱。

(4) 中断：攻击者通过各种方法中断用户的正常通信，达到自己的目的。

(5) 重发：“信息重发”的攻击方式即攻击者截获网络上的密文信息后，并不将其破译，而是将这些数据包再次向有关服务器发送，以实现恶意的目的。

1.1.2 OSI 安全体系结构

OSI(开放系统互连)安全体系结构的研究始于 1982 年，当时 OSI 基本参考模型刚刚确立，其成果标志是 ISO 发布了 ISO 7498—2 标准，作为 OSI 基本参考模型的新补充。1990 年，ITU 决定采用 ISO 7498—2 作为它的 X.800 推荐标准，我国的国际 GB/T 9387.2—1995《信息处理系统 开放系统互连 基本参考模型 第 2 部分：安全体系结构》等同于 ISO/IEC 7498—2。在 ISO 7498—2 中描述了开放系统互连安全的体系结构，提出设计安全的信息系统的基础架构中应该包含 5 种安全服务(安全功能)，能够对这 5 种安全服务提供支持的8类安全机制和普遍安全机制，以及需要进行的 5 种 OSI 安全管理方式。

1. 安全服务

OSI 安全体系结构定义了 5 种安全服务，包括认证服务、访问控制服务、数据完整性服务、数据保密性服务和抗否认性服务。

1）认证服务

认证服务就是提供某个实体的身份保证。它包括对等实体认证和数据源认证两种服务。

对等实体认证服务可以对两个对等实体(用户或进程)在建立连接和开始传输数据时进行身份的合法性和真实性验证，以防止非法用户的假冒和伪造连接初始化攻击。

数据源认证服务可对信息源点进行鉴别，确保数据是由合法用户发出的，以防假冒。

2）访问控制服务

访问控制服务是对某些明确身份的用户限制对某些资源的访问，是实现授权的一种方法。访问控制包括身份验证和权限验证，从而防止未授权用户非法访问网络资源，也防止合法用户越权访问网络资源。

3）数据完整性服务

数据完整性服务防止非法用户对正常数据的变更，如修改、插入、延时或删除，以及在数据交换过程中的数据丢失。数据完整性服务可分为以下 5 种情形：

- 带恢复功能的面向连接的数据完整性；
- 不带恢复功能的面向连接的数据完整性；
- 选择字段面向连接的数据完整性；
- 选择自选无连接的数据完整性；
- 无连接的数据完整性。

4）数据保密性服务

采用数据保密性服务的目的是保证信息的机密性。该服务提供面向连接和无连接两种数据保密方式。保密性服务还提供给用户可选字段的数据保护和信息流安全，即对可能从观察信息流就能推导出的信息提供保护。

5）抗否认性服务

抗否认性服务可防止发送方发送数据后否认自己发送过数据，也可防止接收方接收数据后否认已经接收过数据。它由两种服务组成：一是发送(源点)非否认服务，二是接收(交付)非否认服务。这实际上是一种数字签名服务。

表 1-1 给出了对付典型网络威胁的安全服务，表 1-2 给出了网络各层提供的安全服务。

表 1-1　对付典型网络威胁的安全服务

网络威胁	安全服务
假冒攻击	鉴别服务
非授权侵犯	访问控制服务
窃听攻击	数据机密性服务
完整性破坏	数据完整性服务
服务否认	抗否认性服务
拒绝服务	鉴别服务、访问控制服务和数据完整性服务等

表 1-2 网络各层提供的安全服务

安全服务 \ 网络层次		物理层	数据链路层	网络层	传输层	会话层	表示层	应用层
鉴别	对等实体鉴别			√	√			√
	数据源发鉴别			√	√			√
访问控制				√	√			
数据机密性	连接机密性	√	√	√	√		√	√
	无连接机密性		√	√	√		√	√
	选择字段机密性						√	√
	业务流机密性	√		√				√
数据完整性	可恢复的连接完整性				√			√
	不可恢复的连接完整性			√	√			√
	选择字段的连接完整性							√
	无连接完整性			√	√			√
	选择字段的无连接完整性							√
抗抵赖性	数据源发证明的抗抵赖性							√
	交付证明的抗抵赖性							√

2. 安全机制

OSI 安全体系结构没有详细说明安全服务应该如何来实现。作为指南，它给出了一系列可用来实现这些安全服务的安全机制，如表 1-3 所示。

OSI 安全体系结构的基本机制有加密机制、数字签名机制、访问控制机制、数据完整性机制、认证交换机制、通信业务流填充机制、路由控制和公证机制(把数据向可信第三方注册，以便使人相信数据的内容、来源、时间和传递过程)。

表 1-3 安全服务与安全机制的关系

安全服务 \ 协议层		加密	数字签名	访问控制	数据完整性	认证交换	业务流填充	公证
鉴别	对等实体鉴别	√	√			√		
	数据源发鉴别	√	√					
访问控制				√				
数据机密性	连接机密性	√					√	
	无连接机密性	√					√	
	选择字段机密性	√						
	业务流机密性	√				√	√	
数据完整性	可恢复的连接完整性	√			√			
	不可恢复的连接完整性	√			√			
	选择字段的连接完整性	√			√			
	无连接完整性	√	√		√			
	选择字段的无连接完整性	√	√		√			
抗抵赖性	数据源发证明的抗抵赖性	√	√		√			√
	交付证明的抗抵赖性	√	√		√			√