21世纪高等院校计算机网络工程专业规划教材

网络安全技术理论与实践

廉龙颖　主编
王希斌　王艳涛　刘媛媛　副主编

可下载教学资料
http://www.tup.tsinghua.edu.cn

清华大学出版社

21世纪高等院校计算机网络工程专业规划教材

网络安全技术理论与实践

廉龙颖　主编
王希斌 王艳涛　刘媛媛　副主编

清华大学出版社
北京

内 容 简 介

本书全面地介绍了计算机网络安全的总体情况和发展趋势。全书分为15章，全面讲述网络安全的基础知识（网络安全概述和网络安全编程基础），网络安全攻击技术（黑客与隐藏IP技术，网络扫描与网络监听，网络攻击，网络后门与清除日志，计算机病毒的防治），网络安全防御技术（操作系统安全配置方案，防火墙技术，入侵检测，信息加密与认证技术，无线网络安全）及网络安全工程（网络安全管理，网络安全方案设计）。

本书基本概念清晰，表达深入浅出，内容翔实，重点突出，理论与实践相结合，实用性强，易于教学。

本书可作为信息安全、计算机、网络工程等专业本科生的教科书，也可供从事相关专业教学、科研和工程的人员参考。

图书在版编目（CIP）数据

网络安全技术理论与实践 / 廉龙颖主编. —北京：清华大学出版社，2012.6
（21世纪高等院校计算机网络工程专业规划教材）
ISBN 978-7-302-28192-4

Ⅰ. ①网… Ⅱ. ①廉… 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035143号

责任编辑：高买花　薛　阳
封面设计：常雪影
责任校对：焦丽丽
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
印 装 者：北京国马印刷厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：18.25　　**字　　数**：446千字
版　　次：2012年6月第1版　　**印　　次**：2012年6月第1次印刷
印　　数：1～3000
定　　价：29.00元

产品编号：042886-01

前言

随着计算机网络的发展，网络的开放性、共享性以及互联程度随之扩大，与此同时，网络入侵事件日益增多，网络安全性问题也日益严重。许多大学已设了信息安全专业，或开设了网络安全技术课程，以培养网络安全方面的专业人才。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、信息安全技术等多种学科的综合性科学。总体上，网络安全可以分为网络攻击技术和网络防御技术两大方面。

本书共分为 15 章。第 1 章为网络安全概述，介绍了网络安全的基础知识，重点让读者了解研究网络安全的重要性；第 2 章为网络安全基础，介绍了 TCP/IP 协议、各种网络服务和命令；第 3 章为网络安全编程基础，以多个安全编程实例详细介绍了网络安全编程技术；第 4 章为黑客与隐藏 IP 技术，让读者了解黑客，并详细介绍了网络代理跳板隐藏 IP 技术；第 5 章为网络扫描与网络监听，分别介绍网络扫描和网络监听技术；第 6 章为网络攻击，详细介绍了黑客攻击的各种原理和技术，为读者学习防御技术打下基础；第 7 章为网络后门与清除日志，分别介绍留后门的原理和清除日志的方法；第 8 章为计算机病毒的防治，重点让读者掌握清除病毒的方法；第 9 章为操作系统安全配置方案，介绍了操作系统初级、中级和高级的配置方案；第 10 章防火墙技术，详细介绍了防火墙的功能及配置方法；第 11 章为入侵检测，详细介绍了入侵检测技术；第 12 章为信息加密与认证技术，重点让读者理解加密技术和认证技术；第 13 章为无线网络安全，详细介绍了无线局域网安全技术；第 14 章为网络安全管理，重点介绍网络安全管理知识；第 15 章为网络安全方案设计，以一个网络安全方案实例阐述网络安全方案设计方法。

本书主要有以下特色：

（1）基本概念清晰，表达深入浅出。在基本概念的阐述上，力求准确而精练；在语言的运用上，力求顺畅而自然。

（2）内容翔实，重点突出。本书分为黑客攻击技术和网络安全防御技术两大体系，在网络安全知识体系和知识点的选择上，充分参考了教育部高等学校信息安全类专业教学指导委员会制定的《信息安全类专业课程设置规范》。

（3）理论与实践相结合。网络安全技术是一门实践性很强的学科，因此，全书从网络安全理论和网络安全攻防实践两方面介绍各种网络安全技术，坚持做到理论联系实际。针对每个网络安全技术都设置相应的实践内容，从而使读者能够深入而全面地了解网络安全技术的具体应用，以提高读者在未来的网络安全实践中独立分析问题和解决问题的能力。

本书可作为计算机、信息安全等专业本科生的教材，也可作为广大网络安全工程师、网络管理人员和计算机用户的参考书。通过本书的学习，读者将掌握必要的网络安全知识，并且能够利用这些知识和相应的安全防护工具所提供的安全措施来保护系统。

本书由廉龙颖主编，第 1～7 章由廉龙颖编写，第 8～11 章由王希斌编写，第 12～14 章由王艳涛编写，第 15 章由刘媛媛编写。

由于作者水平有限，编写时间仓促，对书中存在的错误和问题，殷切希望读者批评指正，专业地给予指教。

编　者

2011 年 10 月

于哈尔滨

目 录

第1章 网络安全概述

本章学习目标：

- 了解网络安全的攻防体系；
- 掌握网络安全的层次体系；
- 了解研究网络安全的必要性及社会意义；
- 了解网络安全相关法律法规；
- 掌握实验环境的配置。

1.1 网络安全的攻防体系研究

随着信息化进程的深入和互联网的快速发展，网络化已成为信息化发展的大趋势，信息资源也得到了最大程度的共享。但是，紧随信息化发展而来的网络安全问题也日渐突出，网络安全问题已成为信息时代人类共同面临的挑战。

1.1.1 网络安全是什么

广义上讲，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、信息论等多种学科的综合性科学。

ITU-T X.800 标准对“网络安全（network security）”进行了逻辑上的定义。

（1）安全攻击（security attack）：指损害机构所拥有信息的安全的任何行为。

（2）安全机制（security mechanism）：指设计用于检测、预防安全攻击或者恢复系统的机制。

（3）安全服务（security service）：指采用一种或多种安全机制以抵御安全攻击、提高机构的数据处理系统安全和信息传输安全能力的服务。

在网络安全行业中，一般认为网络安全指的是一种能够识别和消除不安全因素的能力。

1.1.2 网络安全的特征

根据网络安全的定义，如图 1-1 所示，网络安全应具有以下 5 个方面的特征。

1. 保密性

保密性指信息不泄漏给非授权的用户、实体或过程，或供非授权用户、实体或过程利用的特性。从技术上说，任何传输线路，包括电缆（双绞线或同轴电缆）、光缆、微波和卫星，都是可能被窃听的。提供保密性的安全服务取决于若干因素。

（1）需保护数据的位置：数据可能存放在个人计算机或服务器、局域网的线路上，或其他流通介质如软盘、U 盘、光盘等，也可能流经一个完全公开的媒体，如经过互联网或通信卫星。

（2）需保护数据的类型：数据元素可以是本地文件和网络协议所携带的数据和网络协议的信息交换，如一个协议数据单元。

（3）需保护数据的数量或部分：保护整个数据元素、部分数据单元和协议数据单元。

（4）需保护数据的价值：被保护数据的敏感性，以及数据对用户的价值。

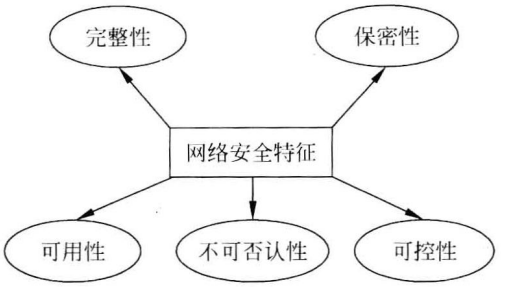

图 1-1　网络安全特征

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。完整性被破坏是计算机网络安全的主要威胁。

破坏信息的完整性既有人为因素，也有非人为因素。非人为因素是指通信传输中的干扰噪声、系统硬件或软件的差错等。人为因素包括有意和无意两种，前者是非法分子对计算机的入侵，合法用户越权对数据进行处理，以及隐藏破坏性程序，如计算机病毒、时间炸弹和逻辑陷阱等；后者是指操作失误或使用不当。

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。

网络可用性还包括在某些不正常条件下继续运行的能力。对网络可用性的破坏，包括合法用户不能正常访问资源和严格时间要求的服务不能得到及时响应。影响网络可用性的因素包括人为与非人为两种。前者是指非法占用网络资源，切断或阻塞网络通信，降低网络性能，甚至使网络瘫痪等；后者是指灾害事故（火、水、雷击等）和系统死锁、系统故障等。

保证可用性的最有效的方法是提供一个具有适当安全服务的安全网络环境。通过使用访问控制阻止未授权的资源访问，利用完整性和保密性服务来防止可用性攻击。访问控制、完整性和保密性成为协助支持可用性安全服务的机制。

（1）避免受到攻击：一些基于网络的攻击旨在破坏、降低或摧毁网络资源。解决办法是加强这些资源的安全保护，使其不受攻击。免受攻击的方法包括修复操作系统和网络配置中的安全漏洞，控制授权实体对资源的访问，防止路由表等敏感网络数据的泄漏等。

（2）避免未授权使用：当资源被使用、占用或过载时，其可用性就会受到限制。如果未授权用户占用了有限的资源，如处理能力、网络带宽和调制解调器连接等，则这些资源

对授权用户就是不可用的，通过访问控制可以限制未授权使用。

（3）防止进程失败：操作失误和设备故障也可导致系统可用性降低。解决方法是使用高可靠性设备、提供设备冗余和提供多路径的网络连接等。

4. 可控性

可控性指对信息的传播及内容具有控制能力，可以控制授权范围内的信息流向及行为方式。

5. 不可否认性

“否认”指参与通信的实体拒绝承认它参加了通信，不可否认性保证信息行为人不能否认其信息行为。不可否认性安全服务提供了向第三方证明该实体确实参与了通信的能力。

数据的接收者提供数据发送者身份及原始发送时间的证据。数据的发送者提供数据已交付接收者的证据。审计服务提供信息交换中各涉及方的可审计性，这种可审计性记录了可用来跟踪某些人的相关事件，这些人应对其行为负责。

不可否认性服务主要由应用层提供。通常用户最关心的是应用程序数据的不可否认性。在低层提供不可否认性功能，仅能证明产生过的连接，而无法将流经该连接的数据同特定的实体相绑定。

1.1.3 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。

1.1.4 保障网络安全的三大支柱

网络安全不仅仅是一个纯技术问题，单凭技术因素确保网络安全是不可能的。保障网络安全无论对一个国家而言还是对一个组织而言都是一个复杂的系统工程，需要多管齐下，综合治理。目前普遍认为网络安全技术、网络安全法律法规和网络安全标准是保障网络安全的三大支柱。

1．网络安全技术

各种网络安全技术的应用主要在技术层面上为网络安全提供具体的保障。目前主要采用的网络安全技术有：网络安全扫描技术、数据加密技术、防火墙技术、入侵检测技术、病毒诊断与防治技术等。尽管网络安全技术的应用在一定程度上对网络的安全起到了很好的保护作用，但它并不是万能的，由于疏于管理等原因而引起的网络安全事故仍然不断发生。

2．网络安全法律法规

国家、地方以及相关部门针对网络安全的需求，制定与网络安全相关的法律法规，从法律层面上来规范人们的行为，使网络安全工作有法可依，使相关违法犯罪能得到处罚，促使组织和个人依法制作、发布、传播和使用网络，从而达到保障网络安全的目的。目前，我国已建立起了基本的网络安全法律法规体系，但随着网络安全形势的发展，网络安全立法的任务还非常艰巨，许多相关法规还有待建立或进一步完善。

3．网络安全标准

建立统一的网络安全标准，其目的是为网络安全产品的制造、安全的信息系统的构建、企业或组织安全策略的制定、安全管理体系的构建以及安全工作评估等提供统一的科学依据。随着网络技术的不断发展和网络安全形势的变化，不但网络安全标准的数量在不断增加，而且许多标准的版本也在不断更新。

1.1.5 网络安全的攻防体系

网络安全的研究内容主要分成两大体系：攻击和防御。该体系研究内容如图 1-2 所示。

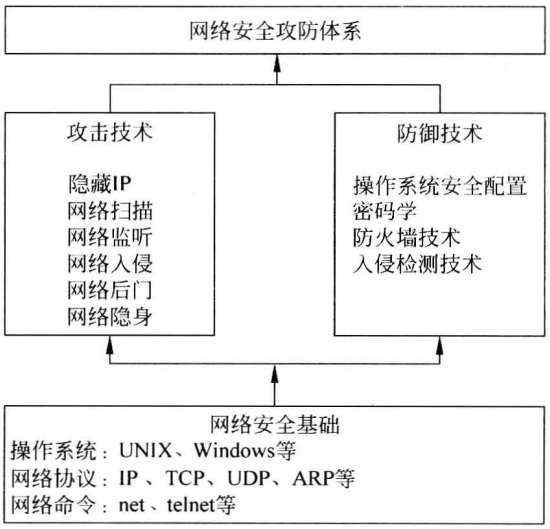

图 1-2　网络安全攻防体系图

作为研究网络安全技术的基础，首先要掌握一些网络基础知识，第一，两大主流操作系统，UNIX 和 Windows 操作系统；第二，常用的网络安全协议，其中包括 IP 、TCP、UDP、ARP 等；第三，常用的网络命令，例如 net、telnet 等。

俗语称“知己知彼，百战不殆”，要想掌握网络安全防御技术，首先要掌握各种攻击