21世纪 高等学校信息安全专业规划教材

网络安全技术与实践

王煜林 田桂丰 主 编
王金恒 刘卓华 副主编

清华大学出版社

21 世纪高等学校信息安全专业规划教材

网络安全技术与实践

王煜林　田桂丰　主　编
王金恒　刘卓华　副主编

清华大学出版社
北 京

内 容 简 介

本书共分10章，主要内容包括网络安全概述、网络攻击与防范、信息加密技术、防火墙技术、计算机病毒及其防治、Windows 2008操作系统的安全、Linux操作系统的安全、VPN技术、入侵检测技术、上网行为管理。本书在强调知识系统性的同时，也注重了全面性，很多技术点都讲解了在Windows、Linux以及Cisco下的不同解决方案。

本书最大的特点是以课业任务的方式来讲解每一个知识点，以帮助读者理解与消化相应的理论知识点，提高读者的兴趣。每一种技术都配备了大量的课业任务。

本书既可以作为应用型本科院校、高职高专院校、民办高校、成人高校、继续教育学院及本科院校的二级学院的教学用书，也可以作为网络工程师、网络安全工程师学习网络安全知识的参考书。

图书在版编目(CIP)数据

网络安全技术与实践/王煜林，田桂丰主编. --北京：清华大学出版社，2013
21世纪高等学校信息安全专业规划教材
ISBN 978-7-302-31652-7

Ⅰ. ①网… Ⅱ. ①王… ②田… 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(2013)第040762号

责任编辑：魏江江　王冰飞
封面设计：杨　兮
责任校对：白　蕾
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**：17.25　　**字　　数**：422千字
版　　次：2013年6月第1版　　**印　　次**：2013年6月第1次印刷
印　　数：1～3000
定　　价：29.00元

产品编号：049505-01

前　言

网络安全技术是计算机科学与技术、网络工程、软件工程等专业的一门必修课，是当今通信与计算机领域的热门课题。Internet 的出现，以及电子商务、网络教育和各种新兴业务的兴起，使人类社会与网络的联系越来越紧密。当网络逐步改变人们的工作方式与生活方式时，利用计算机网络进行犯罪的活动也层出不穷，它已严重地危害了社会的发展与国家安全。因此，网络安全已经成为计算机科学与技术等专业的重要研究领域。

本书的作者都具有多年的网络安全技术教学工作经验，书中安排了非常多的课业任务，凝聚了作者多年以来的教学经验与成果。与同类教材相比，本书具有以下特点：

(1) 知识点以课业任务形式引领，实例丰富。每一章都有大量的课业任务，每一个知识点都是通过课业任务的形式进行讲解，每一个课业任务都有相关的背景知识与相应的操作步骤。把理论知识融入到课业任务中，使读者更容易学习与消化，从而提高读者的学习兴趣。

(2) 强调知识点的系统性。网络安全技术是一门综合性的学科，涉及的学科与技术比较多，本书重点讲解了常见的网络安全技术，如网络攻击与防范、信息加密技术、防火墙技术、VPN 技术、入侵检测技术、上网行为管理、防病毒技术、操作系统安全等，几乎涵盖了网络安全的所有重要知识点。

(3) 强调知识点的全面性。本书在讲解某一项技术时，综合考虑了多平台的技术解决方案，分别讲解了在 Windows 平台、Linux 平台以及 Cisco 平台下的不同解决方案。例如，在讲解 VPN 技术时，讲解了在 Windows 平台下远程访问 VPN 的实现，在 Cisco 平台下站点到站点 VPN 的实现，以及在 Linux 平台下 IPSec VPN 的实现。

本书主要面向应用型本科与高职高专学生，既可以作为高等学校的学生在学习网络安全时的教学辅导用书，也可以作为在校教师的教学参考用书。

本书由王煜林、田桂丰老师担任主编，由王金恒、刘卓华老师担任副主编。全书由 10 章组成，其中第 1 章、第 2 章、第 3 章、第 8 章由王煜林老师编写，第 9 章、第 10 章由田桂丰老师编写，第 4 章由王煜林老师与田桂丰老师共同编写，第 5 章、第 7 章由王金恒老师编写，第 6 章由刘卓华老师编写。

广东技术师范学院天河学院计算机科学与技术系的领导对本书的编写与出版给予了大力的支持，在此表示感谢！在本书的编写过程中，还得到了孔令美、钱宏武、龙君芳等同行的帮助，在此一并表示感谢！

由于作者水平有限，书中难免存在疏漏与不足之处，恳请广大师生与读者给予批评指正，在此深表谢意。我们的邮箱是：43498000@qq.com。

编　者

2013年3月

目　录

第1章 网络安全概述

随着信息科技的迅速发展以及计算机网络的普及，计算机网络已深入到国家的政府、军事、金融、商业等诸多领域，可以说网络无处不在。它在实现信息交流共享、为人们带来极大便利和丰富社会生活的同时，出于政治、经济、文化等利益的需求或者好奇心的驱动，网络攻击事件层出不穷，且有愈演愈烈之势，轻者给个人或者机构带来信息损害、经济利益损失，重者将会影响国家的政治、经济和文化安全。因此，加强对信息网络安全技术的研究，无论是对个人还是组织、机构，甚至国家、政府都有非同寻常的意义。

学习目标：

- 了解网络安全的现状。
- 掌握网络安全的定义、基本要素。
- 掌握网络安全相关技术。
- 掌握网络安全实验平台的搭建。

课业任务：

本章通过3个课业任务，学习在各种环境下网络安全实验平台的搭建。

课业任务 1-1

Bob是WYL公司的网络安全运维工程师，现在在家里办公，不能连接互联网，他想完成一个由3台计算机组成网络的安全实验。Bob使用虚拟机实现3台计算机互连。

能力观测点

VMware虚拟机的网络连接方式；使用Host-only实现虚拟机中的客户机Windows Server 2008、Red Hat Enterprise Linux 6与物理机Windows XP互相通信。

课业任务 1-2

Bob为了保证公司用户接入网络的安全，他在公司接入层交换机上开启了端口安全，只允许授权的PC接入到交换机从而访问互联网。当非授权的PC接入交换机后，交换机就启用端口安全机制，关闭此接口，直到管理员手动启用此接口。

能力观测点

Cisco Packet Tracer模拟器的使用；端口安全的配置与测试。

课业任务 1-3

Bob为了保证远程管理设备的安全，他采用SSH远程管理方法来替代明文传送数据包的Telnet。Bob在路由器上启用了SSH服务。

能力观测点

GNS(Graphical Network Simulator)模拟器的使用；路由器上SSH服务的配置与测试。

1.1 网络安全概况

1.1.1 网络安全现状

现在，人们的生活已经与网络息息相关，如网上购物、网上银行、网上政务、网上交流、网上教学等。网络是一把双刃剑，给人们的生活带来了便利的同时，也给人们的生活带来了安全威胁。中国互联网络信息中心(CNNIC)于 2012 年 7 月 19 日发布的《中国互联网发展状况调查报告》统计数据显示，截至 2012 年 6 月底，中国网民数量达到 5.38 亿，互联网普及率为 39.9%，如图 1.1 所示。可以说，网络已经无处不在，已经深入到了国家的政治、经济、文化以及社会生活。正因为如此，网络安全问题也日益突出。

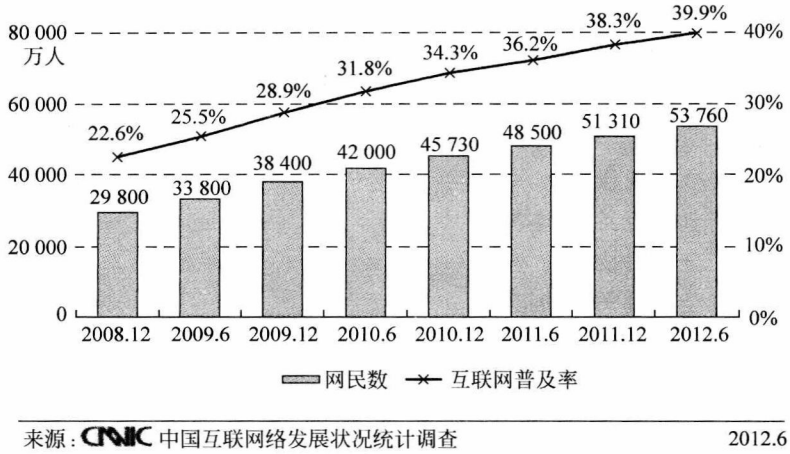

图 1.1 中国网民规模和互联网普及率

由于互联网不断深入人们的生活，网络安全事件层出不穷，愈演愈烈，以下是近几年发生的网络安全重大事件。

(1) 2012 年 2 月 4 日，黑客集团 Anonymous 公布了一份来自 2012 年 1 月 17 日美国 FBI 和英国伦敦警察厅的工作通话录音，时长 17 分钟，主要内容是双方讨论如何寻找证据和逮捕 Anonymous、LulzSec、Antisec、CSL Security 等黑客的方式。目前，FBI 已经确认了该通话录音的真实性，安全研究人员已经开始着手解决电话会议系统的漏洞问题。

(2) 2011 年几乎称得上是互联网的“资料泄露年”。3 月份，RSA 遭到黑客攻击，获取认证的 SecurID 相关信息被窃取；4 月份，“索尼被黑”事件导致黑客从索尼在线 PlayStation 网络中窃取了 7700 万客户的信息，包括信用卡账号，这一黑客攻击事件导致索尼被迫关闭了该服务并损失了 1.7 亿美元；而 CSDN 泄密事件中，珍爱网、开心网、猫扑、天涯、智联招聘、酷 6 网等知名网站的用户数据被盗取，数千万用户密码信息暴露在互联网上，同时大量用户发现微博账号、支付宝账号被盗。

(3) 2010 年 7 月 25 日，“维基解密”通过英国《卫报》、德国《明镜》和美国《纽约时报》公布了 92 000 份美军有关阿富汗战争的军事机密文件。10 月 23 日，“维基解密”公布了

391 832 份美军关于伊拉克战争的机密文件。11 月 28 日，“维基解密”泄露了 25 万份美国驻外使馆发给美国国务院的秘密文传电报。“维基解密”是美国乃至世界历史上最大规模的一次泄密事件，其波及范围之广、涉及文件之众均史无前例。该事件引起了世界各国政府对信息安全工作的重视和反思。据美国有线电视新闻网 12 月 13 日报道，为防止军事机密泄露，美国军方已下令禁止全军使用 USB 存储器、CD 光盘等移动存储介质。

(4) 2010 年 9 月，奇虎 360 针对腾讯公司的 QQ 聊天软件发布了“360 隐私保护器”和“360 扣扣保镖”两款网络安全软件，并称其可以保护 QQ 用户的隐私和网络安全。腾讯公司认为奇虎 360 的这一做法严重危害了腾讯的商业利益，并称“360 扣扣保镖”是“外挂”行为。随后，腾讯公司在 11 月 3 日宣布将停止对装有 360 软件的计算机提供 QQ 服务。由此而引发了“3Q 大战”，同时引起了 360 软件与其他公司类似产品的一系列纷争，最终演变成了互联网行业中的一场混战。最终，“3Q 大战”在国家相关部门的强力干预下得以平息，“360 扣扣保镖”被召回，QQ 与 360 恢复兼容。但此次事件对广大终端用户造成了恶劣影响和侵害，并由此引发了公众对于终端安全和隐私保护的困惑及忧虑却远没有消除。

(5) 2009 年的 519 断网事件是由于几家网游私服之间的恶性竞争引起的，其中一家以网络攻击的手段向为对方解释域名的 DNS 服务器 DNSPod 发动 DDoS(分布式拒绝服务)攻击。其本意只想让 DNSPod 宕机，让对手的网游玩家不能访问其游戏服务器。可未曾想到，就是这样的一次网络攻击行为，却最终演变成造成广西、江苏、海南、安徽、甘肃和浙江电信宽带用户网络断网的严重网络安全事件。

以上只是近年来影响比较大的网络安全事件，诸如此类的安全事件非常多，每天都有新的漏洞与病毒在恶意地破坏网络系统。在众多的网络安全事件中，主要网络攻击行为为 DDoS 攻击、信息泄露、网络钓鱼、蠕虫病毒、软件漏洞等。ANVA(中国反网络病毒联盟)周报在 2012 年第 48 期的互联网网络安全指数整体评价中指出，境内感染网络病毒的主机数约为 217.9 万个，较上周数量环比减少了约 13.1%；新增网络病毒家族 5 个，较上周新增数量增加了 4 个；境内被篡改政府网站数量为 48 个，占境内被篡改网站数量的 7.3%。图 1.2 所示为 2012 年 10 月 29 日至 11 月 4 日的活跃互联网病毒类型分布情况。从图中可以看出，主要的互联网病毒是后门工具、木马程序、蠕虫、黑客工具、流氓软件等。

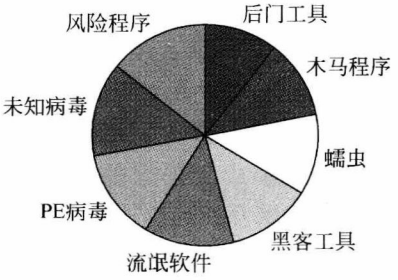

图 1.2　2012.10.29—2012.11.4 病毒类型分布情况

除了以上的病毒外，软件漏洞也给网络带来了许多安全隐患。2012 年，CNVD(国家计算机网络应急技术处理协调中心)漏洞周报第 43 期(2012 年 10 月 29 日至 11 月 04 日)共收录了 113 个漏洞。其中，操作系统漏洞 4 个，应用程序漏洞 39 个，Web 应用漏洞 65 个，网络设备漏洞 5 个，分布情况如图 1.3 所示。

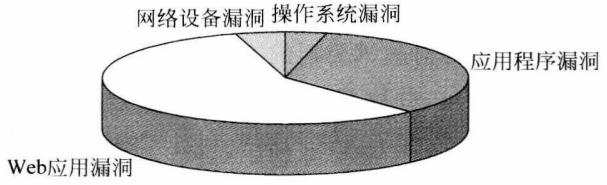

图 1.3　2012.10.29—2012.11.04 漏洞分布情况

如图 1.3 所示，Web 应用漏洞最多，其次是应用程序漏洞。大软件厂商成为黑客们最“钟爱”的对象，时常会有超级危险的安全问题被黑客暴露出来，就像衣服有了破洞，从而迫使软件厂商不得不经常给自己的产品打补丁。其中，有 3 家因为补丁数目超多而被誉为软件界的三大“乞丐”，分别是 Adobe、微软和 Java。图 1.4 所示为访问 Java 漏洞制作的网页，弹出的计算器可运行任意程序。

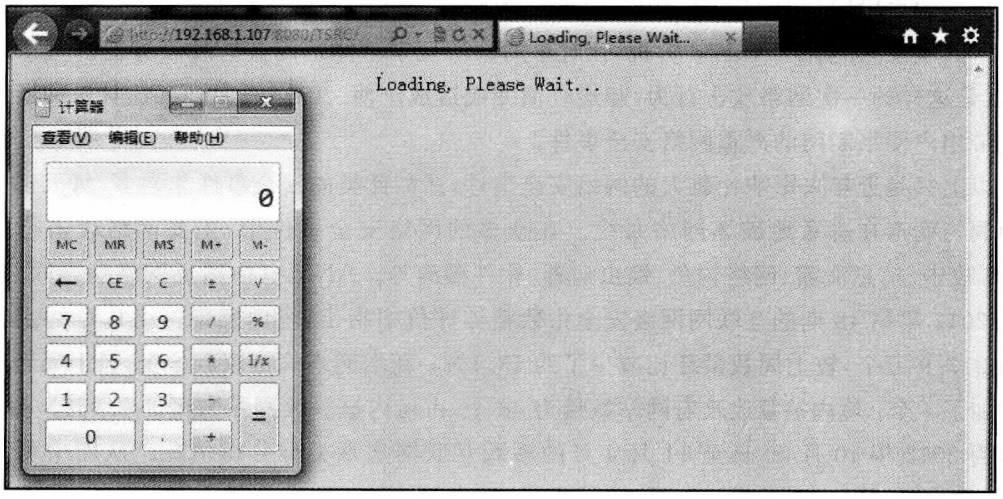

图 1.4　Java 漏洞网页

据了解，在 Adobe 系列中，仅 Flash 插件就占领了 2011 年十大重磅漏洞的 4 个席位，近期流行的 PDF 漏洞也让用户非常担心，作为占有率最高的操作系统厂商——微软也难逃黑客的“爱慕”，各种系统漏洞补丁都有可能被黑客利用。而随着 Java 用户群的逐渐壮大，3 亿安装量吸引了黑客的目光，使其渐渐成为黑客的“新宠”，2011 年 12 月初，一则披露 Oracle 公司 Java Applet Rhino 脚本引擎存在远程执行代码高危漏洞的消息在网络上掀起轩然大波便是证明。

网络钓鱼(Phishing)也是近年来兴起的另一种新型网络攻击手段。黑客建立一个网站，通过模仿银行、购物网站、炒股网站、彩票网站等，诱骗用户访问。由于成本低，收益大，

钓鱼网站不仅种类多了，数量也迅速增长。2011 年，除了传统的假淘宝网站、假 QQ 网站、假网上银行网站、六合彩钓鱼网站等之外，黑客又发展假 sina 网站、假机票网站、假火车票网站、假药品网站等。可以说，随着互联网应用的发展，尤其是电子商务的进一步发展，“网络钓鱼”正在高速壮大，网民们的生活则需要“步步小心”，如图 1.5 所示。

图 1.5　网络钓鱼更加猖狂

2006 年，第 38 届世界电信日的主题是 Promoting Global Cybersecurity（推进全球网络安全），人们已经意识到，网络安全问题与大家的生活已息息相关，全球网络安全的问题不能依靠一个国家、一个企业或一种技术来解决，这是一项牵涉到政府、企业、个人和国际合作的复杂工程，需要各方面的共同努力。

1.1.2　网络安全的定义

网络安全是指在分布式网络环境中对信息载体（处理载体、存储载体、传输载体）和信息的处理、传输、存储、访问提供安全保护，以防止数据、信息内容遭到破坏、更改、泄露，并防止网络服务中断、拒绝服务、被非授权使用和篡改。从广义上来说，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。

对网络安全内涵的理解会随着“角色”的变化而有所不同，而且在不断地延伸和丰富。例如，从用户的角度来说，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，避免他人利用窃听、冒充、篡改、抵赖等手段侵犯其利益。

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进行的访问、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、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，避免机要信息泄露，避免对社会产生危害，避免对国家造成巨大损失。

可见，网络安全的内涵与其保护的信息对象有关，但本质都是在信息的安全期内保证在网络上传输或静态存放时允许授权用户访问，而不被未授权用户非法访问。

1.1.3 网络安全的基本要素

网络安全的基本要素主要包括5个方面。

1. 机密性

机密性主要是防止信息在存储或传输的过程中被窃取。防止数据被查看最有效的方法就是加密，在现代加密体制中，最典型的加密算法是对称加密算法与非对称加密算法。

2. 完整性

信息只能被得到允许的人修改，并且能够被判别该信息是否已被篡改。主要是通过哈希算法来保证数据的完整性，典型的哈希算法有MD5与SHA1。

3. 可用性

只有授权者才可以在需要时访问该数据，而非授权者应被拒绝访问。

4. 可控性

对各种访问网络的行为进行监视、审计，控制授权范围内的信息流向及行为方式。

5. 不可抵赖性

数据的发送方与接收方都无法对数据传输的事实进行抵赖，主要是通过数字签名来实现不可否认性。

1.1.4 网络安全的标准

国际标准化组织(ISO)、国际电气技术委员会(IEC)及国际电信联盟(ITU)所属的电信标准化组织(ITU. TS)在安全需求服务分析指导、安全技术机制开发、安全评估标准等方面制订了一些标准草案。另外，IETF也有9个功能组讨论网络安全并制定相关标准。

目前，国内外主要的安全评价标准有以下几个。

1. 美国TCSEC

该标准由美国国防部制定，将安全分为4个方面，即安全政策、可说明性、安全保障和文档。标准将上述4个方面又分为7个安全级别，从低到高依次为D、C1、C2、B1、B2、B3和A级。

2. 欧洲ITSEC

该标准叙述了技术安全的要求，把保密作为安全增强功能。与TCSEC不同的是，ITSEC把完整性、可用性作为与保密同等重要的因素。ITSEC定义了从E0级(不满足品质)到E6级(形式化验证)的7个安全等级，对于每个系统，安全功能可分别定义。ITSEC预定义了10种功能，其中前5种与TCSEC中的C1～B3级非常相似。

3. 联合公共准则CC

它的目的是把已有的安全准则结合成一个统一的标准。该计划从1993年开始执行，1996年推出第一版，1998年推出第二版，现已成为ISO标准。CC结合了TCSEC及ITSEC的主要特征，强调将安全的功能与保障分离，并将功能需求分为9类63族，将保障分为7类29族。

4. ISO安全体系结构标准(ISO7498—2—1989)

该标准在描述基本参考模型的同时，提供了安全服务与有关机制的一般描述，确定在参考模型内部可以提供这些服务与机制的位置。

5. 中华人民共和国国家标准GB17895. 1999《计算机信息系统安全保护等级划分准则》

该标准将信息系统安全分为5个等级，分别是自主保护级、系统审计保护级、安全标记