高职高专计算机教学改革新体系规划教材

计算机网络安全技术案例教程

耿 杰 主编

清华大学出版社

高职高专计算机教学改革新体系规划教材

计算机网络安全技术案例教程

耿杰 主 编

钱亮 张宏宪 田岭 白悍东 副主编

清华大学出版社
北京

内 容 简 介

本书以 Windows Server 2003 为平台，通过实用的网络安全案例介绍计算机网络安全技术，使学生可以对网络安全知识学以致用。在内容的选取、组织与编排上，强调技术性、先进性、实用性，淡化理论，突出实践，强调应用。

本书共分为 9 章，内容如下：网络安全概述，通信协议与安全，数据加密技术，Windows Server 2003 的安全，防火墙技术，入侵检测技术，网络病毒的防范与清除，网络攻防技术，Web 安全技术。

本书既可以作为高职高专院校网络相关专业及电子商务等专业学习计算机网络安全技术的教材，也可以单独作为实验指导用书；同时，它还是一本实用的技术指导书，可以作为社会培训教材。

图书在版编目(CIP)数据

计算机网络安全技术案例教程/耿杰主编. --北京：清华大学出版社，2013
高职高专计算机教学改革新体系规划教材
ISBN 978-7-302-31213-0

Ⅰ. ①计… Ⅱ. ①耿… Ⅲ. ①计算机网络－安全技术－高等职业教育－教材 Ⅳ. ①TP383.08

中国版本图书馆 CIP 数据核字(2013)第 001762 号

责任编辑：陈砺川
封面设计：傅瑞学
责任校对：刘　静
责任印制：宋　林

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，010-62795764

印 刷 者：三河市君旺印装厂
装 订 者：三河市新茂装订有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：16.75　　**字　　数**：386 千字
版　　次：2013 年 10 月第 1 版　　**印　　次**：2013 年 10 月第1次印刷
印　　数：1～3000
定　　价：33.00 元

产品编号：050613-01

前言

FOREWORD

编者在多年教学和实践经验的基础上，结合当前计算机网络安全技术的新成果，对计算机网络安全技术相关知识作了系统的介绍。本书以案例为依托，结合目前企业对网络安全技术的需求，主要介绍了以下内容：网络安全概述；通信协议与安全；数据加密技术；Windows Server 2003 的安全；防火墙技术；入侵检测技术；网络病毒的防范与清除；网络攻防技术；Web 安全技术。

本书具有如下特色。

以适应高职高专教学改革的需要为目标，充分体现高职高专特色，努力从内容到形式上有所创新和突破，其最大特点就是以企业需求为导向，讲究实用性。

在内容选取上，坚持集先进性、科学性和实用性为一体，尽可能选取最新、最实用的技术，满足以“提高学生能力为主”的高职高专教学的需要。

在考虑教材内容深浅程度时，把握理论够用、侧重实践、由浅入深的原则，以使学生分层分步骤掌握所学的知识。

在教材结构的安排上，采用实例引导和任务驱动模式作为教材编写的主干线，从知识—案例—练习—实训，逐渐展开内容，通过案例使知识具体化，增强对网络安全技术的感性认识，通过练习和实训来巩固和深化所学的知识，最后达到学习知识、培养能力的目的。本书案例丰富、典型，针对性强，能够很好地满足读者对知识和技能的需求。

本书既可以作为高职高专院校网络相关专业及电子商务等专业学习计算机网络安全技术的教材，也可以作为实验指导用书，同时也可以作为社会培训班用书。

在本书的编写过程中，编者参阅了大量的网上资料和出版的论文、教材、专著等，在此向这些作品的作者表示深深的敬意和感谢！

本书由耿杰担任主编并负责全书的统稿工作，钱亮、张宏宪、田岭、白悍东作为本书的副主编做了很多重要的工作，另外，彭庆红也参与了本书的编写。

由于作者水平有限，书中难免有不妥和错误之处，恳请广大读者指正。

目录

CONTENTS

第1章 网络安全概述

Chapter 1

知识目标

- 理解网络安全的定义。
- 掌握网络面临的各种安全威胁。
- 了解产生网络安全威胁的原因。
- 了解计算机系统的安全级别。

技能目标

- 能识别网络威胁的类别。
- 能使用网络工具对计算机系统进行漏洞扫描。
- 掌握常用 DOS 命令的操作方法。

随着网络技术的不断发展，网络在人们生活中已经占有一席之地，为人们的生活带来了极大的方便。然而，网络也不是完美无缺的，它在给人们带来惊喜的同时，也带来了威胁。计算机犯罪、黑客、有害程序和后门等问题严重威胁着网络的安全。目前，网络安全问题已经在许多国家引起了普遍关注，成为当今网络技术的一个重要研究课题。

1.1 什么是网络安全

目前，Internet 几乎覆盖了世界各地，容纳了数十万个网络，为几十亿用户提供了形式多样的网络与信息服务。除了广泛应用的 Web 网页、E-mail、新闻论坛等文本信息的交流与传播之外，网络电话、网络传真、视频等通信技术都在迅猛地发展。在信息化社会中，计算机网络将在政治、军事、金融、商业、交通、电信、文教等方面发挥越来越大的作用。社会对网络的依赖日益增强。人们依靠计算机网络系统接收和处理信息，实现相互间的联系和对目标的管理、控制。通过网络交流信息、获得信息已成为现代信息社会的一个主要特征。网络正改变着人们的工作方式和生活方式。

科技进步在造福人类的同时，也带来了新的危害。随着网络的开放性、共享性和互联程度的扩大，特别是 Internet 的出现，网络变得越来越重要，对社会的影响也越来越大，随之而来的是利用计算机网络犯罪的情况越来越严重，已经严重地危害着社会的发展和国家的安全。

1989 年 10 月，有人为了抗议钚驱动的伽利略探测器的发射而制造 WANK(Worms Against Nuclear Killers)蠕虫入侵 NASA(美国宇航局)，这是历史上有记载的第一次系统入侵，造成了约 50 万美元的损失。

1996 年 8 月 14 日，美国发生一起计算机病毒入侵计算机网络的事件，几千台计算机被病毒感染，Internet 不能被正常访问。政府不得不立即做出反应，国防部成立了计算机快速行动小组。这次病毒事件导致的直接经济损失超过 1 亿美元。

1994 年底，俄罗斯黑客弗拉米尔与其同伙从圣彼得堡的一家小软件公司的联网计算机上向美国 CITYBANK 银行发动了一连串的攻击，通过电子转账方式，从 CITYBANK 银行在纽约的计算机主机里窃取了 1100 万美元。

2000 年 1 月，一个昵称为 Maxim 的黑客侵入 CDUniverse. com 购物网站并窃取了 30 万份信用卡资料。

2003 年 3 月 21 日，黑客侵入了江苏某信息网的多台服务器，破译了密码数据库，获得了网络工作人员的口令和 300 多个合法用户的账号与密码，并将这些账号与密码公布于众。

2008 年 2 月，一黑客利用无线刷卡设备的漏洞入侵了美国两家大型连锁超市 Hannaford 和 Sweetbay，盗窃了 1800 份完整信用卡资料和 420 万个信用卡的部分资料。

事实上，以上这些网络入侵事件只是实际发生的网络入侵事件中非常微小的一部分，有相当多的网络入侵或攻击并没有被发现，或者出于各种各样的原因未被公开。据统计，商业信息被窃取的事件在每月以 260%的速度增加。社会上每公开报道一次网络入侵事件的背后，有无数例网络入侵事件是不被公众所知的。

面对越来越严重的计算机网络安全的威胁，必须采取措施来保证计算机网络的安全。但是现有的计算机网络大多数在设计的开始都忽略了安全问题。即使考虑了安全问题，大部分都是把安全机制建立在物理安全上。随着网络互联程度的扩大，这种安全机制对于网络环境来讲很脆弱。同时，目前网络上使用的协议，如 TCP/IP 协议，在制定之初也没有把安全考虑在内，所以网络协议本身就是不设防的，TCP/IP 协议中存在很多的安全问题，不能满足网络安全的要求。另外，网络的开放性和资源共享也是安全问题的一个主要根源，解决这个问题主要依赖于加密、网络用户身份鉴别、存取控制策略等技术手段。

一个安全的网络体系至少应包括三类措施，即法律措施、技术措施、政策措施。面对危害计算机网络安全的种种威胁，仅仅利用物理上和政策上的手段是十分有限和困难的，因此，也应采用逻辑上的措施，即研究开发有效的网络安全技术，例如，安全协议、密码技术、数字签名、防火墙、安全管理、安全审计等，以防止网络上传输的信息被非法窃取、篡改、伪造，保证其保密性和完整性；防止非法用户的侵入，限制网络上用户的访问权限，保证信息存放的私有性。除了私有性和完整性之外，一个安全的计算机网络还必须考虑通信双方身份的真实性和信息的可用性。

计算机网络安全的目的是要保证网络上数据存储和传输的安全性。国内外很多研究机构为了解决这个问题做了大量的工作，主要有数据加密、身份认证、数字签名、防火墙、安全审计、安全管理、安全内核、安全协议、IC 卡、拒绝服务、网络安全性分析、网络信息安全监测和信息安全标准化等方面的研究。

1.1.1 计算机网络安全

计算机网络安全是指保持网络中的硬件、软件系统正常运行，使它们不因自然和人为的因素而被破坏、更改和泄露。网络安全主要包括物理安全、软件安全、信息安全和运行安全四个方面。

1. 物理安全

物理安全包括硬件、存储媒体和外部环境的安全。硬件是指网络中的各种设备和通信线路，如主机、路由器、服务器、工作站、交换机、电缆等；存储媒体包括磁盘、光盘等；外部环境则主要指计算机设备的安装场地、供电系统。保障物理安全，就是要保护这些硬件设施能够正常工作而不被损害。

2. 软件安全

软件安全是指网络软件及各个主机、服务器、工作站等设备所运行的软件的安全。保障软件安全，就是保护网络中的各种软件能够正常运行而不被修改、破坏和使用。

3. 信息安全

信息安全是指网络中所存储和传输数据的安全，主要体现在信息隐蔽性和防修改的能力上。保障信息安全，就是保护网络中的信息不被非法修改、复制、解密、使用等，也是保障网络安全最根本的目的。

4. 运行安全

运行安全指网络中的各个信息系统能够正常运行并能正常地通过网络交流信息。保障运行安全，就是通过对网络系统中的各种设备运行状况进行监测，发现不安全因素时，及时报警并采取相应措施，消除不安全状态以保障网络系统的正常运行。

网络安全的目的是为了确保网络系统的保密性、完整性和可用性。保密性要求只有授权用户才能访问网络信息；完整性要求网络中的数据保持不被意外或恶意地改变；可用性指网络在不降低使用性能的情况下仍能根据授权用户的需要提供资源服务。

1.1.2 网络安全的特征

由于网络安全受到威胁的多样性、复杂性及网络信息、数据的重要性，在设计网络系统时，应该努力达到安全目标。一个安全的网络具有下面五个特征：可靠性、可用性、保密性、完整性和不可抵赖性。

1. 可靠性

可靠性是网络安全最基本的要求之一，是指系统在规定条件下和规定时间内完成规定功能的概率。如果网络不可靠，经常出问题，这个网络就是不安全的。目前，对于网络可靠性的研究主要偏重于硬件可靠性方面。研制高可靠性硬件设备，采取合理的冗余备

份措施是最基本的可靠性对策。但实际上有许多故障和事故，与软件可靠性、人员可靠性和环境可靠性有关。如人员可靠性在通信网络可靠性中起着重要作用。有关资料表明，系统失效中很大一部分是由人为因素造成的。

2. 可用性

可用性是可被授权实体访问并按需求使用的特性，即当需要时能否存取所需的信息。网络最基本的功能是向用户提供所需的信息和通信服务，而用户的通信要求是随机的、多方面的，有时还要求具有时效性。网络必须随时满足用户通信的要求。从某种意义上讲，可用性是可靠性的更高要求，特别是在重要场合下，特殊用户的可用性显得十分重要。为此，网络需要采用科学、合理的网络拓扑结构，必要的冗余、容错和备份措施及网络自愈技术、分配配置和负荷分担、各种完善的物理安全和应急措施等，从满足用户需求出发，保证通信网络的安全。在网络环境下，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。

3. 保密性

保密性指防止信息泄露给非授权个人或实体。信息只为授权用户使用，保密性是对信息的安全要求。它是在可靠性和可用性的基础上，保障网络中信息安全的重要手段。对于敏感用户信息的保密，是人们研究最多的领域。由于网络信息会成为黑客、计算机犯罪、病毒，甚至信息战的攻击目标，已受到了人们越来越多的关注。

4. 完整性

完整性也是面向信息的安全要求。它是指信息不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等操作破坏的特性。它与保密性不同，保密性是防止信息泄露给非授权的人，而完整性则要求信息的内容和顺序都不受破坏和修改。用户信息和网络信息都要求完整性，例如，对于涉及金融的用户信息，如果用户账目被修改、伪造或删除，将带来巨大的经济损失。网络信息一旦被破坏，严重的还会造成通信网络的瘫痪。

5. 不可抵赖性

不可抵赖性也称不可否认性，是面向通信双方（人、实体或进程）信息真实的安全要求。它包括收发双方均不可抵赖。随着通信业务的不断扩大，电子贸易、电子金融、电子商务和办公自动化等许多信息处理过程都需要通信双方对信息内容的真实性进行认同，为此，应采用数字签名、认证，数据完备、鉴别等有效措施，以实现信息的不可抵赖性。

网络的安全不仅仅是防范窃密活动，其可靠性、可用性、完整性和不可抵赖性应作为与保密性同等重要的安全目标来实现。我们应从观念上、政策上做出必要的调整，全面规划和实施网络信息的安全。

1.2 网络安全面临的威胁

1.2.1 网络内部威胁

1. 计算机系统的脆弱性

计算机系统的脆弱性主要来自计算机操作系统的不安全性，在网络环境下，还来源于网络通信协议的不安全性。计算机系统有其自身的安全级别，有的计算机操作系统属于D级，这一级别的操作系统基本没有安全防护措施，它就像一个门窗大开的屋子，如DOS、Windows 3.x、Windows 95等操作系统，它们只能用于一般的桌面计算机系统，而不能用于安全性要求高的服务器的操作系统。UNIX系统和Windows NT达到了C2级别，其安全性远远高于Windows 95操作系统，而且主要用于服务器上。但这种操作系统仍然存在安全漏洞，因为这两种系统都存在超级用户，UNIX中是root，而Windows NT中是Administrator，如果入侵者得到了超级用户口令，整个系统将完全受控于入侵者，这样系统将面临巨大的危险。现在，人们正在研究一种新型的操作系统，在这种操作系统中没有超级用户，也就不会存在超级用户带来的问题。现在很多操作系统都使用静态口令，但口令还是有很大破解可能性的，而且不好的口令维护制度会导致口令丢失。口令丢失也就意味着安全系统的全面崩溃。

世界上没有能长久运行的计算机系统，计算机系统可能会因硬件故障或软件原因而停止运行或发生运行错误，或被入侵者利用并造成损失。硬盘故障、电源故障和主板芯片故障等都是人们应经常考虑的硬件故障问题。软件原因可能存在于操作系统中，更多的是存在于应用软件中。

2. 网络内部的威胁

对网络内部的威胁主要来自网络内部的用户，这些用户试图访问那些不允许使用的资源和服务器。这种威胁可以分为如下两种情况。

(1) 有意的安全破坏，入侵者的攻击和计算机犯罪就是属于这一类。这是计算机网络所面临的最大威胁，此类威胁还可以分为主动攻击和被动攻击两种情况，主动攻击是指计算机网络的内部用户以各种方式有选择地破坏信息的有效性和完整性，而被动攻击则是在不影响网络正常工作的情况下，进行信息截获、窃取、破译等，目的是为了获得重要机密信息。

(2) 由于用户安全意识差造成的无意识的操作失误，使系统或网络发生故障或崩溃。如操作员安全配置不当造成的安全漏洞或隐患，用户安全意识不强，用户口令选择不慎或不恰当，用户将自己的账号保护不严或与别人共享等，都会对网络安全带来威胁和隐患，或者被非法入侵者加以利用，从而造成对系统的危害。

1.2.2 网络外部威胁

除了受到来自网络内部的安全威胁外，网络还受到来自外界的各种各样的威胁。网

络系统受到的威胁是多样的，因为在网络系统中可能存在许多种类的计算机和操作系统，采用统一的安全措施是不容易的，也是不可能的，而对网络进行集中安全管理则是一种好的方案。

安全威胁可以归结为物理威胁、网络威胁、身份鉴别、编程、系统漏洞等方面。

1. 物理威胁

物理安全是指保护计算机硬件和存储介质等设备和工作程序不遭受损失。常见的物理安全威胁有偷窃、垃圾搜寻和间谍活动等。物理安全是计算机系统和网络操作系统安全的最重要的方面。

办公室的计算机是偷窃者的主要目标之一。由于计算机或网络服务器中存储的数据信息的价值远远超过设备的价值，计算机偷窃行为对用户的损失可能成倍于被偷的设备的价值。因此，必须采取严格的防范措施以确保计算机设备不会被偷窃。入侵者可能会潜入计算机房，偷取计算机或计算机里的机密信息，也可能化装成计算机维修人员，趁管理员不注意时进行偷窃。当然，也可能是内部职员窃取他们不应该看到的信息，并把信息散布出去或卖给竞争对手。

千万不要小看了搜寻垃圾。在商业竞争中，有些人专门会搜寻竞争对手扔下的垃圾，以寻找一些机密信息。办公室的工作人员可能会把一些没经过任何安全处理的打印错误的文件扔进废纸篓，而这些文件就有可能落到竞争对手的手中，这样，机密信息便泄露了。

间谍活动是人们不能忽略的一种因素，现在商业间谍很多，而且一些商业机构可能会为击败对手而采取任何不道德的手段，有时政府机关也有可能卷入这种间谍活动当中。

2. 网络威胁

计算机网络的发展和使用对数据信息造成了新的安全威胁。在计算机网络中存在电子窃听，分布式计算机系统的特征使各种分离的计算机通过一些媒介相互连接在一起，进行相互通信，而且局域网一般是广播式的，只要把网卡模式设置成混合模式，网络上人人都可以收到发向任何人的信息。当然，也可以通过加密来解决这个问题，但目前强大的加密技术还没有在网络上广泛使用，况且加密也是有可能被破解的。

网络设备也可以造成网络的安全威胁。我国的很多个人网络用户都是通过调制解调器用电话线等方式拨号接入 Internet 或单位的局域网的，因为调制解调器也存在安全问题，入侵者可能通过电话线入侵到用户的网络中。

在 Internet 上还存在很多电子欺骗的现象，而这种电子欺骗的形式也是多种多样的，如一个公司可能会谎称一个站点是其公司的网站。在网络通信中，有的人可能冒充别人或冒充从另外一台机器访问某站点等，这样会很难辨别用户的真实身份。

3. 身份鉴别

目前，身份鉴别普遍存在于计算机系统当中，实现的方式各种各样，有的功能十分强大，有的则比较脆弱。其中，口令就是一种比较脆弱的身份鉴别手段，它的功能不是很强，但因为它实现起来比较简单，所以还是被广泛采用。计算机系统中的身份鉴别存在口令

圈套、口令破解和算法缺陷等安全威胁。

口令圈套是一种十分高明的诡计，它是一种靠欺骗来获取口令的手段。如登录欺骗，具体是写出一个运行起来像登录屏幕一样的代码模块，把它插入登录过程之前，这样，用户就会把用户名和登录口令告知程序，这个程序会把用户名和口令保存起来。除此之外，该代码还会告诉用户登录失败，并启动真正的登录程序，这样用户就不容易发现这个欺骗。

还有一种得到口令的方式是用密码字典或其他工具软件来暴力破解口令，有的用户选用的口令十分脆弱，如一个人的生日、电话号码、名字或单词等，这样攻击者就很容易强行破解。因此，系统管理员应对用户的口令进行严格审查，通常可以利用一些工具软件来检查口令是否达到系统管理的要求和规定。

口令输入后要正常工作必须满足一定的条件，当条件发生变化时，其口令算法程序就可能工作不正常。即当人们移植一种算法时，这种算法可能在人们工作环境下存在漏洞，这就是口令算法缺陷带来的安全隐患。

4. 编程

编程威胁主要有计算机病毒和特洛伊木马等。编程就是通过编制程序代码实施对系统的破坏。计算机病毒就是一种能进行自我复制的程序代码，它可以像生物病毒一样传染别的完好的程序。计算机病毒具有一定的破坏性，破坏性大小不一样，小的只是显示一些信息，影响用户使用计算机，而大的可能会让整个系统瘫痪。现在，Internet 上有很多种类的病毒，这些病毒在网络上不断地传播，严重危害 Internet 的安全。它可能通过不同的方式进入用户的计算机系统或网络系统，如下载软件、Java Applet 程序、ActiveX 和电子邮件等。

现在，在桌面系统中流行一种宏病毒，可以破坏 Word 文档，这种病毒存在于宏操作的软件中，如 Microsoft 的 Word 和 Excel 等软件。

逻辑炸弹是一种恶意代码，它可以让用户的系统瞬间崩溃，还会格式化硬盘或删除系统文件等。特洛伊木马也是一种恶意代码，但它和逻辑炸弹不同，它会把自己伪装成一个很正常的程序，在用户不知道的情况下破坏系统，具有很大的破坏性。

5. 系统漏洞

系统漏洞是指应用软件或操作系统软件在逻辑设计上的缺陷或在编写时产生的错误，这个缺陷或错误可以被不法者或者黑客利用，通过植入木马、病毒等方式来攻击或控制整个计算机，从而窃取其中的重要资料和信息，甚至破坏计算机系统。

漏洞影响到的范围很广，包括系统本身及其支撑软件、网络客户和服务器软件、网络路由器和安全防火墙等。换言之，在这些不同的软、硬件设备中都可能存在不同的安全漏洞问题。在不同种类的软、硬件设备，同种设备的不同版本之间，由不同设备构成的不同系统之间，以及同种系统在不同的设置条件下，都会存在不同的安全漏洞问题。