高职高专计算机任务驱动模式教材

网络安全技术项目化教程

黄林国 章仪 主编

清华大学出版社

高职高专计算机任务驱动模式教材

网络安全技术项目化教程

黄晓国 等编 主

清华大学出版社
北京

内 容 简 介

本书基于“项目引导、任务驱动”的项目化教学方式编写而成，体现“基于工作过程”、“教、学、做”一体化的教学理念。本书内容划分为11个工程项目，具体内容包括：认识计算机网络安全技术、Windows系统安全加固、网络协议与分析、计算机病毒及防治、密码技术、网络攻击与防范、防火墙技术、入侵检测技术、VPN技术、Web安全、无线网络安全。每个项目案例按照“提出问题”→“分析问题”→“解决问题”→“拓展提高”四部曲展开。读者能够通过项目案例完成相关知识的学习和技能的训练，每个项目案例来自企业工程实践，具有典型性、实用性、趣味性和可操作性。

本书可作为高等职业院校和高等专科院校“网络安全技术”课程的教学用书，也可作为成人高等院校、各类培训、计算机从业人员和爱好者的参考用书。

图书在版编目（CIP）数据

网络安全技术项目化教程/黄林国主编. —北京：清华大学出版社，2012.8
（高职高专计算机任务驱动模式教材）
ISBN 978-7-302-29447-4

Ⅰ. ①网… Ⅱ. ①黄… Ⅲ. ①计算机网络—安全技术—高等职业教育—教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2012)第161334号

责任编辑：张龙卿
封面设计：何凤霞
责任校对：李　梅
责任印制：张雪娇

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**：19.75　　**字　数**：477千字
版　　次：2012年8月第1版　　**印　次**：2012年8月第1次印刷
印　　数：1～3000
定　　价：38.00元

产品编号：046783-01

前　言

从1999年开始，高等学校连续进行了十几年的大规模扩招，大学教育也开始由精英教育转为大众化教育。随着教学对象、教学目标和教学环境的转变，传统的教学内容、教学方法和教学手段已不再适合高职教育的需要。

计算机网络的出现改变了人们使用计算机的方式，也改变了人们的学习、工作和生活方式。计算机网络给人们带来便利的同时，也带来了保证网络安全的巨大挑战。据媒体统计，截至2012年3月底，我国网民规模已达到5.27亿人，互联网普及率为39.4%。有52%的网民曾遭遇过网络安全事件，有21.2%的网民曾遭受直接经济损失，有4.4%的网民个人计算机未安装任何安全软件，不足8%的手机网民安装手机安全防护软件，这些进一步说明，普及全民的网络安全意识仍然任重道远。

“网络安全技术”已成为高职院校计算机及相关专业的重要必修课程。本书根据高等职业教育的特点，基于“项目引导、任务驱动”的项目化教学方式编写而成，体现“基于工作过程”、“教、学、做”一体化的教学理念，将全书内容划分为11个工程项目，具体内容包括：认识计算机网络安全技术、Windows系统安全加固、网络协议与分析、计算机病毒及防治、密码技术、网络攻击与防范、防火墙技术、入侵检测技术、VPN技术、Web安全、无线网络安全。本书具有以下特点。

(1) 体现“项目引导、任务驱动”教学特点。从实际应用出发，从工作过程出发，从项目出发，采用“项目引导、任务驱动”的方式，通过“提出问题”→“分析问题”→“解决问题”→“拓展提高”四部曲展开。在宏观教学设计上突破以知识点的层次递进为理论体系的传统模式，将职业工作过程系统化，以工作过程为参照系，按照工作过程来组织和讲解知识，培养学生的职业技能和职业素养。

(2) 体现“教、学、做”一体化的教学理念。以学到实用技能、提高职业能力为出发点，以“做”为中心，“教”和“学”都围绕着“做”，在学中做，在做中学，从而完成知识学习、技能训练和提高职业素养的教学目标。

(3) 本书体例采用项目、任务形式。全书设有11个工程项目，每一个项目再明确若干任务。教学内容安排由易到难、由简单到复杂，层次推进，循序渐进。学生能够通过项目学习，完成相关知识的学习和技能的训练。每个项目来自企业工程实践，具有典型性和实用性。

(4) 项目/任务的内容体现趣味性、实用性和可操作性。趣味性使学生始终保持较高的学习兴趣和动力;实用性使学生能学以致用;可操作性保证每个项目/任务能顺利完成。本书的讲解力求贴近口语,让学生感到易学、乐学,在宽松环境中理解知识、掌握技能。

(5) 紧跟行业技术发展。网络安全技术发展很快,本书着力于当前主流技术和新技术的讲解,与行业联系密切,使所有内容紧跟行业技术的发展。

(6) 符合高职学生认知规律,有助于实现有效教学,提高教学的效率、效益、效果。本书打破传统的学科体系结构,将各知识点与操作技能恰当地融入各个项目/任务中,突出现代职业教育的职业性和实践性,强化实践,培养学生实践动手能力,适合高职学生的学习特点,在教学过程中注意情感交流,因材施教,调动学生的学习积极性,提高教学效果。

(7) 本书中相关任务操作对实验环境的要求比较低,采用常见的设备和软件即可完成,便于实施。为了方便操作和保护系统安全,本书中的大部分任务操作均可在 Windows Server 2003 虚拟机中完成,部分任务操作要在 Windows Server 2000 虚拟机中完成,所用的工具软件均可在互联网上下载。

本书由黄林国、章仪任主编,其中项目 1～项目 10 由黄林国编写,项目 11 由章仪编写,全书由黄林国统稿。参加编写的还有娄淑敏、曾希君、王振邦、叶敏、凌代红、张丽君、黄倩、陈伟钱、张瑛、叶婉秋、王亚君、李育喜等。在编写过程中,参考了大量的书籍和互联网上的资料,在此,谨向这些书籍和资料的作者表示感谢。

为了便于教学,本书提供的 PPT 课件等教学资源可以从清华大学出版社网站(http://www.tup.com.cn)的下载区免费下载。

由于编者水平有限,书中难免存在不当和疏漏之处,敬请读者批评指正。联系方式 huanglgvip@21 cn.com。

编　者

2012 年 6 月

目 录

项目 1　认识计算机网络安全技术

1.1　项 目 提 出

据国外媒体报道，全球计算机行业协会（CompTIA）近日评出了“全球最急需的 10 项 IT 技术”，结果安全和防火墙技术排名首位。

据 CompTIA 近日公布的《全球 IT 技术状况》报告显示，安全/防火墙/数据隐私类技术排名首位，而网络技术位居第二。

全球最急需的 10 项 IT 技术：

（1）安全/防火墙/数据隐私类技术。

（2）网络/网络基础设施。

（3）操作系统。

（4）硬件。

（5）非特定性服务器技术。

（6）软件。

（7）应用层面技术。

（8）特定编程语言。

（9）Web 技术。

（10）RF 移动/无线技术。

由上可见，排名第一的就是安全问题，这说明安全方面的问题是全世界都亟须解决的问题，可想而知我们所面临的网络安全状况有多尴尬。

1.2　项 目 分 析

计算机网络近年来得到了飞速的发展，在网络高速发展的过程中，网络技术的日趋成熟使得网络连接更加容易，人们在享受网络带来便利的同时，网络的安全也日益受到威胁。

互联网和网络应用以飞快的速度不断发展，网络应用日益普及并更加复杂，网络安全问题是互联网和网络应用发展中面临的重要问题。网络攻击行为日趋复杂，各种方法相互融合，使网络安全防御更加困难。黑客攻击行为组织性更强，攻击目标从单纯地追求“荣耀感”向获取多方面实际利益的方向转移，网上木马、间谍程序、恶意网站、网络仿冒等的出现和日趋泛滥；智能手机、平板计算机等无线终端的处理能力和功能通用性提高，使其日趋接近个

人计算机，针对这些无线终端的网络攻击已经开始出现，并将进一步发展。

总之，网络安全问题变得更加错综复杂，影响将不断扩大，很难在短期内得到全面解决。安全问题已经摆在了非常重要的位置上，网络安全如果不加以防范，会严重影响网络的应用。

1.3 相关知识点

1.3.1 网络安全概述

1. 网络安全的重要性

尽管网络的重要性已经被广泛认同，但对网络安全的忽视仍很普遍，缺乏网络安全意识的状况仍然十分严峻。不少企事业单位极为重视网络硬件的投资，但没有意识到网络安全的重要性，对网络安全的投资较吝啬。这也使得目前不少网络信息系统都存在先天性的安全漏洞和安全威胁，有些甚至产生了非常严重的后果。下面是近年来发生的一些重大网络信息安全事件。

1995 年，米特尼克闯入许多计算机网络，窃取了两万个信用卡号，他曾闯入“北美空中防务指挥系统”，破译了美国著名的“太平洋电话公司”在南加利福尼亚州通信网络的“改户密码”，入侵过美国 DEC 等 5 家大公司的网络，造成 8000 万美元的损失。

1999 年，台湾大学生陈盈豪制造的 CIH 病毒在 4 月 26 日发作，引起全球震撼，有 6 千多万台计算机受到伤害。

2002 年，黑客用 DDos 攻击影响了 13 个根 DNS 中的 8 个，作为整个 Internet 通信路标的关键系统遭到严重的破坏。

2006 年，“熊猫烧香”木马致使我国数百万计算机用户受到感染，并波及周边国家。2007 年 2 月，“熊猫烧香”制作者李俊被捕。

2008 年，一个全球性的黑客组织利用 ATM 欺诈程序在一夜之间从世界 49 个城市的银行中盗走了 900 万美元。

2009 年，韩国遭受有史以来最猛烈的一次黑客攻击。韩国总统府、国会、国情院和国防部等国家机关，以及金融界、媒体和防火墙企业网站遭受攻击，造成网站一度无法访问。

2010 年，“维基解密”网站在《纽约时报》、《卫报》和《镜报》配合下，在网上公开了多达 9.2万份的驻阿美军秘密文件，引起轩然大波。

2011 年，堪称中国互联网史上最大泄密事件发生。12 月中旬，CSDN 网站用户数据库被黑客在网上公开，大约 600 万个注册邮箱账号和与之对应的明文密码泄露。2012 年 1 月 12 日，CSDN 泄密的两名嫌疑人已被刑事拘留。其中一名为北京籍黑客，另一名为外地黑客。

以上仅仅是一些个案，事实上，这样的案例不胜枚举，而且计算机犯罪案件有逐年增加的趋势。据美国的一项研究显示，全球互联网每 39 秒就发生了一次黑客事件，其中大部分

黑客没有固定的目标。

因此，网络系统必须有足够强大的安全体系，无论是局域网还是广域网，无论是单位还是个人，网络安全的目标是全方位防范各种威胁以确保网络信息的保密性、完整性和可用性。

2. 网络安全的现状

现今 Internet 环境正在发生着一系列的变化，安全问题也出现了相应的变化，主要反映在以下几个方面。

(1) 网络犯罪成为集团化、产业化的趋势。从灰鸽子病毒案例可以看出，木马从制作到最终盗取用户信息甚至财物，渐渐成为一条产业链。

(2) 无线网络、智能手机成为新的攻击区域，新的攻击重点。随着无线网络的大力推广，3G 网络使用人群的增多，使用的用户群体也在不断地增加，手机病毒、手机恶意软件呈现快速增长的趋势。

(3) 垃圾邮件依然比较严重。虽然经过这么多年的垃圾邮件整治，垃圾邮件现象得到明显改善，例如美国有相应的立法来处理垃圾邮件，但是在利益的驱使下，垃圾邮件仍然影响着每个人的邮箱使用。

(4) 漏洞攻击的爆发时间变短。从这几年发生的攻击来看，不难发现漏洞攻击的时间越来越短，系统漏洞、网络漏洞、软件漏洞等被攻击者发现并利用的时间间隔在不断地缩短，很多攻击者都是通过这些漏洞来攻击网络的。

(5) 攻击方的技术水平要求越来越低。现在有很多黑客网站免费提供了许多攻击工具，利用这些工具可以很容易地实施网络攻击。

(6) Dos(Deny of Service)攻击更加频繁。由于 Dos 攻击更加隐蔽，难以追踪到攻击者，大多数攻击者采用分布式的攻击方式和跳板攻击方法，这种攻击更具有威胁性，攻击更加难以防范。

(7) 针对浏览器插件的攻击。插件的性能不是由浏览器来决定的，浏览器的漏洞升级并不能解决插件可能存在的漏洞。

(8) 网站攻击，特别是网页被挂木马。大多数用户在打开一个熟悉的网站，比如自己信任的网站，但是这个网站被挂木马，在不经意间木马将会安装在自己的计算机中，这是现在网站攻击的主要模式。

(9) 内部用户的攻击。现今企事业单位的内部网与外部网的联系越来越紧密，来自内部用户的威胁也不断地表现出来。来自内部攻击的比例在不断上升，变成内部网络的一个防灾重点。

据我国国家计算机网络应急技术处理协调中心(简称 CNCERT/CC)统计，2010 年，CNCERT 共处理各类网络安全事件 3236 件，较 2009 年的 1176 件增长了 175%。CNCERT 处理的网络安全事件的类型构成如图 1-1 所示[①]，主要有漏洞、恶意代码、网页挂马等。

① 来自 CNCERT/CC 2010 年中国互联网络安全报告。

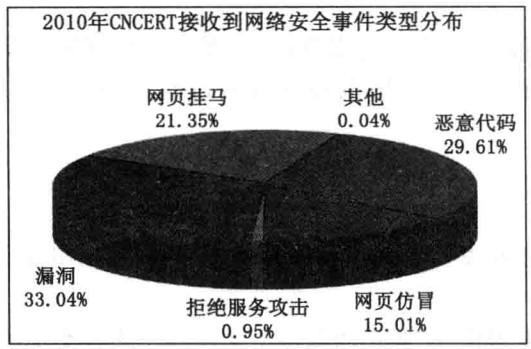

图 1-1　2010 年 CNCERT 接收到网络安全事件类型分布

3. 网络安全的定义

网络安全是指计算机及其网络系统资源和信息资源不受自然与人为有害因素的威胁和危害，即是指计算机、网络系统的硬件和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、泄露，确保系统能连续可靠正常地运行，使网络服务不中断。

计算机网络安全从其本质上来讲就是系统上的信息安全。计算机网络安全是一门涉及计算机科学、网络技术、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。

从广义来说，凡是涉及计算机网络上信息的保密性、完整性、可用性、可控性和不可否认性的相关技术和理论都是计算机网络安全的研究领域。

(1) 保密性

保密性是指网络信息不被泄露给非授权的用户或过程，即信息只为授权用户使用。即使非授权用户得到信息也无法知晓信息的内容，因而不能使用。

(2) 完整性

完整性是指维护信息的一致性，即在信息生成、传输、存储和使用过程中不发生人为或非人为的非授权篡改。

(3) 可用性

可用性是指授权用户在需要时能不受其他因素的影响，方便地使用所需信息，即当需要时能否存取所需的信息。例如，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。

(4) 可控性

可控性是指对网络系统中的信息传播及具体内容能够实现有效控制，即网络系统中的任何信息要在一定传输范围和存放空间内可控。

(5) 不可否认性

不可否认性是指保障用户无法在事后否认曾经对信息进行的生成、签发、接收等行为，一般通过数字签名来提供不可否认服务。

从网络运行和管理者角度来说，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，它们希望对非法的、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，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。

网络安全问题，应该像每家每户的防火、防盗问题一样，做到防患于未然。甚至不会想到自己也会成为目标的时候，威胁就已经出现了，一旦发生，常常措手不及，造成极大的损失。

4. 网络安全的主要威胁

网络系统的安全威胁主要表现在主机可能会受到非法入侵者的攻击，网络中的敏感数据有可能泄露或被修改，从内部网向公共网传送的信息可能被他人窃听篡改等。典型的网络安全威胁如表 1-1 所示。

表 1-1　典型的网络安全威胁

威　胁	含　义
窃听	网络中传输的敏感信息被窃听
重传	攻击者事先获得部分或全部信息，以后将此信息发送给接收者
伪造	攻击者将伪造的信息发送给接收者
篡改	攻击者对合法用户之间的通信信息进行修改、删除、插入，再发送给接收者
非授权访问	通过假冒、身份攻击、系统漏洞等手段获取系统访问权，从而使非法用户进入网络系统读取、删除、修改、插入信息等
拒绝服务访问	攻击者通过某种方法使系统响应减慢甚至瘫痪，阻止合法用户获得服务
行为否认	通信实体否认已经发生的行为
旁路控制	攻击者发掘系统的缺陷或安全脆弱性
电磁/射频截获	攻击者从电子或机电设备所发出的无线射频或其他电磁辐射中提取信息
人员疏忽	已授权人为了自己的利益或由于粗心将信息泄露给未授权人

5. 影响网络安全的主要因素

影响网络安全的因素有很多，归纳起来主要有以下一些因素。

（1）开放性的网络环境

网络特点正如一句非常经典的话所描述的："Internet 的美妙之处在于你和每个人都能互相连接，Internet 的可怕之处在于每个人都能和你互相连接。"

Internet 是一个开放性的网络，是跨越国界的，这意味着网络的攻击不仅来自本地网络的用户，也可以来自 Internet 上的任何一台机器。Internet 是一个虚拟的世界，无法得知联机的另一端是谁。在这个虚拟的世界里，已经超越了国界，某些法律也受到了挑战，因此网络安全面临的是一个国际化的挑战。

网络建立初期只考虑方便性、开放性，并没有考虑总体安全构架，任何一个人或者团体

都可能接入，因而网络所面临的破坏和攻击可能是多方面的。例如，可能是对物理传输线路的攻击，可能是对操作系统漏洞的攻击，可能是对网络通信协议的攻击，也可能是对硬件的攻击等。网络安全已成为信息时代人类共同面临的挑战。

(2) 操作系统的漏洞

漏洞是可以在攻击过程中利用的弱点，它可以是软件、硬件、程序缺点、功能设计或者配置不当等造成的。黑客或入侵者会研究分析这些漏洞，加以利用而获得侵入和破坏的机会。

网络连接离不开网络操作系统，操作系统可能存在各种漏洞，有很多网络攻击的方法都是从寻找操作系统的漏洞开始的。

① 系统模型本身的漏洞。这是系统设计初期就存在的，无法通过修改操作系统程序的源代码来修补。

② 操作系统程序的源代码存在漏洞。操作系统也是一个计算机程序，任何一个程序都可能存在漏洞，操作系统也不例外。例如，冲击波病毒针对的是 Windows 操作系统的 RPC 缓冲区溢出漏洞。

③ 操作系统程序配置不当。许多操作系统的默认配置的安全性较差，进行安全配置比较复杂并且需要一定的安全知识，许多用户并没有这方面的能力，如果没有正确配置这些安全功能，会造成一些系统的安全缺陷。

(3) TCP/IP 协议的缺陷

一方面，该协议数据流采用明码传输，且传输过程无法控制，这就为他人截取、窃听信息提供了机会；另一方面，该协议在设计时采用协议簇的基本体系结构，IP 地址作为网络节点的唯一标识，不是固定的且不需要身份认证。因此攻击者就有了可乘之机，他们可以通过修改或冒充他人的 IP 地址进行信息的拦截、窃取和篡改等。

(4) 人为因素

在计算机使用过程中，使用者的安全意识缺乏、安全管理措施不到位等，通常是网络安全的一个重大隐患。例如，隐秘性文件未设密，操作口令的泄露，重要文件的丢失等都会给黑客提供攻击的机会。对于系统漏洞的不及时修补以及不及时防病毒都可能会给网络安全带来影响。

1.3.2 网络安全所涉及的内容

网络安全是一门交叉学科，除了涉及数学、通信、计算机等自然科学外，还涉及法律、心理学等社会科学，是一个多领域的复杂系统。一般的，把网络安全涉及的内容分为物理安全、网络安全、系统安全、应用安全、管理安全 5 个方面，如图 1-2 所示。

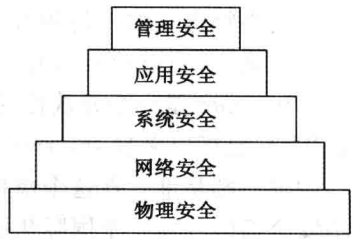

图 1-2 网络安全所涉及的内容

1. 物理安全

物理安全也称实体安全，是指保护计算机设备、设施(网络及通信线路)免遭地震、水灾、火灾等自然灾害和环境事故(如电磁污染等)，以及人为操作失误及计算机犯罪行为导致的破坏。保证计算机信息系统各种设备的物理安全，是整个计算机信息系统安全的前提。物理安全主要包括以下 3 个

方面。

(1) 环境安全:对系统所有环境的安全保护,如区域保护(电子监控)和灾难保护(灾难的预警、应急处理、恢复等)。

(2) 设备安全:主要包括设备的防盗、防毁(接地保护)、防电磁信息辐射泄露、防止线路截获、抗电磁干扰及电源保护等。

(3) 媒体安全:包括媒体数据的安全及媒体本身的安全。

2. 网络安全

网络安全主要包括网络运行和网络访问控制的安全,如表 1-2 所示。

表 1-2　网络安全的组成

网络安全	局域网、子网安全	访问控制(防火墙)
		网络安全检测(入侵检测系统)
	网络中数据传输安全	数据加密(VPN 等)
	网络运行安全	备份与恢复
		应急
	网络协议安全	TCP/IP
		其他协议

在网络安全中,在内部网与外部网之间,可以设置防火墙来实现内外网的隔离和访问控制,是保护内部网安全的最主要的措施,同时也是最有效、最经济的措施之一。网络安全检测工具通常是一个网络安全性的评估分析软件或硬件,用此类工具可以检测出系统的漏洞或潜在的威胁,以达到增强网络安全性的目的。

备份是为了尽可能快地全面恢复运行计算机系统所需要的数据和系统信息。备份不仅在网络系统硬件出现故障或人为操作失误时起到保护作用,也在入侵者非授权访问或对网络攻击及破坏数据完整性时起到保护作用,同时也是系统灾难恢复的前提之一。

3. 系统安全

系统安全的组成如表 1-3 所示。

表 1-3　系统安全的组成

系统安全	操作系统安全	反病毒
		系统安全检测
		入侵检测(监控)
		审计分析
	数据库系统安全	数据库安全
		数据库管理系统安全

人们一般对网络和操作系统的安全很重视,而对数据库的安全不够重视,其实数据库系