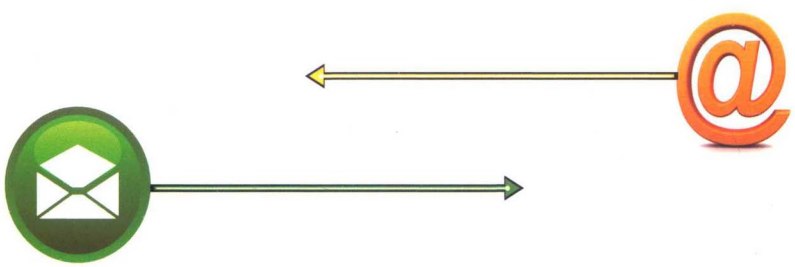
高等院校计算机任务驱动教改教材

网络信息安全基础

黄林国 主 编 林仙土 陈 波 陈 平 副主编



清华大学出版社

高等院校计算机任务驱动教改教材

网络信息安全基础

黄林国 主 编 林仙土 陈 波 陈 平 副主编

清华大学出版社
北京

内容简介

本书系统全面地讲解了网络信息安全的基础概念和基本原理。全书共有11章，主要以Windows 7和Windows Server 2008为平台，内容包括网络信息安全概述、Windows Server 2008系统安全、网络协议与分析、计算机病毒与木马防护、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。每章中均包含了技能实训，便于读者操作并提升技能。

本书可作为应用型本科、高职高专计算机相关专业“网络信息安全基础”课程的教材，也可作为各类培训班、计算机从业人员和计算机爱好者的参考用书。

图书在版编目(CIP)数据

网络信息安全基础/黄林国主编. —北京：清华大学出版社，2018
(高等院校计算机任务驱动教改教材)
ISBN 978-7-302-48758-6

Ⅰ. ①网… Ⅱ. ①黄… Ⅲ. ①计算机网络－信息安全－高等学校－教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2017)第272238号

责任编辑：张龙卿
封面设计：徐日强
责任校对：李　梅
责任印制：沈　露

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,010-62770175-4278

印 装 者：北京泽宇印刷有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　张**：23.25　　**字　数**：563千字
版　　次：2018年1月第1版　　**印　次**：2018年1月第1次印刷
印　　数：1～2500
定　　价：59.00元

产品编号：077364-01

前　言

计算机网络的出现改变了人们使用计算机的方式，也改变了人们学习、工作和生活的方式。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。据统计，截至 2016 年 12 月底，我国网民规模已达到 7.31 亿人，其中手机网民规模达 6.95 亿人，互联网普及率为 53.2%，其中农村地区互联网普及率为 33.1%。81.64%的网民不注意定期更换密码，其中遇到问题才更换密码的占 64.59%，从不更换密码的占 17.05%；75.93%的网民存在多账户使用同一密码的问题；80.21%的网民随意连接公共免费 WiFi；83.48%的网民网上支付行为存在安全隐患；36.96%的网民对二维码“经常扫，不考虑是否安全”；55.18%的网民曾遭遇网络诈骗。这些进一步说明，普及全民的网络安全意识仍然任重道远。

“网络信息安全基础”已成为高等院校计算机及相关专业的重要必修课程。全书共有 11 章，主要以 Windows 7 和 Windows Server 2008 为平台，分别介绍了网络信息安全的相关知识。每章中均包含了技能实训，便于读者操作并提升技能。

本书中相关实验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，本书中的大部分实验操作均可在 Windows Server 2008/Windows 7 虚拟机中完成，部分实验操作要在 Windows 2000 Server 虚拟机中完成，所用的工具软件均可在互联网上下载。

本书由黄林国担任主编并统稿，林仙土、陈波、陈平担任副主编。参加编写的还有解卫华、娄淑敏、黄倩、王振邦、凌代红、张丽君、陈邦荣、林龙、滕圣敏、夏文明、沈爱莲、张康、牟维文、陈波等。在本书的编写过程中，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，本书提供了 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/）免费下载使用。

由于编者水平有限，书中难免存在疏漏，敬请读者批评指正。联系方式为 huanglgvip@21cn.com。

编　者

2017 年 10 月

目 录

第 1 章　网络信息安全概述

(1) 掌握网络信息安全的定义和主要威胁。
(2) 了解网络信息安全的现状和主要影响因素。
(3) 了解网络信息安全所涉及的主要内容。
(4) 了解 PDRR 模型、安全策略设计原则和网络信息安全保障技术。
(5) 了解网络信息安全标准。
(6) 掌握 VMware 虚拟机技术的使用方法。

1.1　网络信息安全简介

计算机网络是信息社会的基础，已经进入社会的各个角落，经济、文件、军事和社会生活越来越多地依赖计算机网络。然而，开放性的网络在给人们带来巨大便利的同时，其安全性如何保证？因此，计算机网络的安全性成为信息化建设的一个核心问题。

计算机网络中存储、传输和处理的信息多种多样，许多是敏感信息，甚至是国家机密，例如，政府宏观调控决策、商业经济信息、股票证券、科研数据等重要信息。由于网络安全漏洞等原因，可能会造成信息泄露、信息窃取、数据篡改、数据破坏、计算机病毒发作、恶意信息发布等事件，由此造成的经济损失和社会危害难以估量。互联网已经渗透到生活的方方面面。习近平主席曾说过，“没有网络安全，就没有国家安全”。在频发的安全事件催化下，网络信息安全已经上升至国家战略高度。

1.1.1　网络信息安全的重要性

尽管网络的重要性已经被广泛认同，但对网络信息安全的忽视仍很普遍，缺乏网络信息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，但没有意识到网络信息安全的重要性，对网络信息安全的投资较少。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，偷窃了 2 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，中国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破坏。

2006年，“熊猫烧香”木马致使我国数百万台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。

2013年6月，前中情局(CIA)职员爱德华·斯诺登曝光美国国家安全局的“棱镜”项目，该项目为秘密项目，过去6年间，美国国家安全局和联邦调查局通过进入微软、谷歌、苹果、雅虎等九大网络巨头的服务器，监控美国公民的电子邮件、聊天记录、视频及照片等秘密资料。

2014年12月25日，乌云漏洞报告平台称，大量12306用户数据在互联网疯传，内容包括用户账号、明文密码、身份证号码、手机号码和电子邮箱等。这次事件是黑客首先通过收集互联网某游戏网站，以及其他多个网站泄露的用户名和密码信息，然后通过撞库[①]的方式利用12306安全机制的欠缺获取了13万多条用户数据。

2015年12月23日，乌克兰发生了一次影响很大的通过有组织、有预谋的定向网络攻击，致使乌克兰境内近1/3的地区持续断电的安全事件。

2016年5月7日，根据路透社报道，黑客在黑市上交易高达3亿条被盗的邮件账户用户名和密码，其中，5700万条为俄罗斯Mail.ru邮件账户、4000万条为雅虎邮件账户、3300万条为Hotmail邮件账户，以及240万条为Gmail邮件账户。另外，还包含成千上万的德国和中国的电子邮件账户，以及数以千计的涉及美国银行业、制造业和零售业公司员工的用户名和密码。

2017年5月12日，一款名为“想解密”(又称“想哭”)的勒索病毒在全球范围内疯狂传播。欧洲刑警组织5月14日称，已经有上百个国家和地区，数十万台计算机被感染，而后需要支付高额赎金，才能解锁计算机中被感染的文件。我国部分高校和大型企业的内网也遭受到病毒的侵袭。

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39s就发生一次黑客事件，其中大部分黑客

① 撞库是指黑客利用从某些网站或渠道获取的用户账号和密码，在其他网站上进行登录尝试。这主要是由于目前有相当一部分互联网用户喜欢在不同网站上使用统一的用户名和密码。

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，网络信息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。

1.1.2　网络信息安全的现状

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，4G 网络使用人群的增多，使用的用户群体也在不断增加，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。从近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，拒绝服务)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在不断地表现出来。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。

据国家互联网应急中心发布的《2016 年中国互联网网络安全报告》中显示，2016 年，国家互联网应急中心共接收境内外报告的网络安全事件 125 660 起，较 2015 年的 126 916 起下降 1.0%。其中，境外报告的网络安全事件数量为 474 起，较 2015 年下降 14.0%。接收的网络安全事件中，数量排名前三位的类型分别是网页仿冒事件(占 42.3%)、漏洞事件(占 24.6%)和恶意程序事件(占 12.0%)。

1.1.3 网络信息安全的定义

网络信息安全是陆、海、空、天之上的第五维国家安全边界。网络信息安全是一个关系国家主权、安全、社会稳定、民族文化继承和发扬的重要问题。其重要性，正随着全球信息化步伐的加快越来越重要。

网络信息安全是指计算机及其网络系统资源和信息资源不受自然和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。

网络信息安全从其本质上来讲就是系统上的信息安全。网络信息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网络信息安全的研究领域。

1）保密性

保密性是指网络信息不被泄露给非授权的用户、实体或过程，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。这一目标是对信息系统的总体可靠性要求。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

可控性是指对流通在网络系统中的信息传播及具体内容能够实现有效控制的特性，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。除了采用常规的传播站点和传播内容监控这种形式之外，最典型的如密码的托管政策，当加密算法交由第三方管理时，必须严格按规定可控执行。

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、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。

网络信息安全问题，应该像每家每户的防火、防盗问题一样，做到防患于未然。

1.1.4　网络信息安全的主要威胁

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。典型的网络信息安全威胁如表 1-1 所示。

表 1-1　典型的网络信息安全威胁

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
拒绝服务攻击	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被授权人

1.1.5　影响网络信息安全的主要因素

影响网络信息安全的因素有很多，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可以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，因此网络信息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以接入，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。网络信息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，它可以是由软件、硬件、程序缺陷、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。