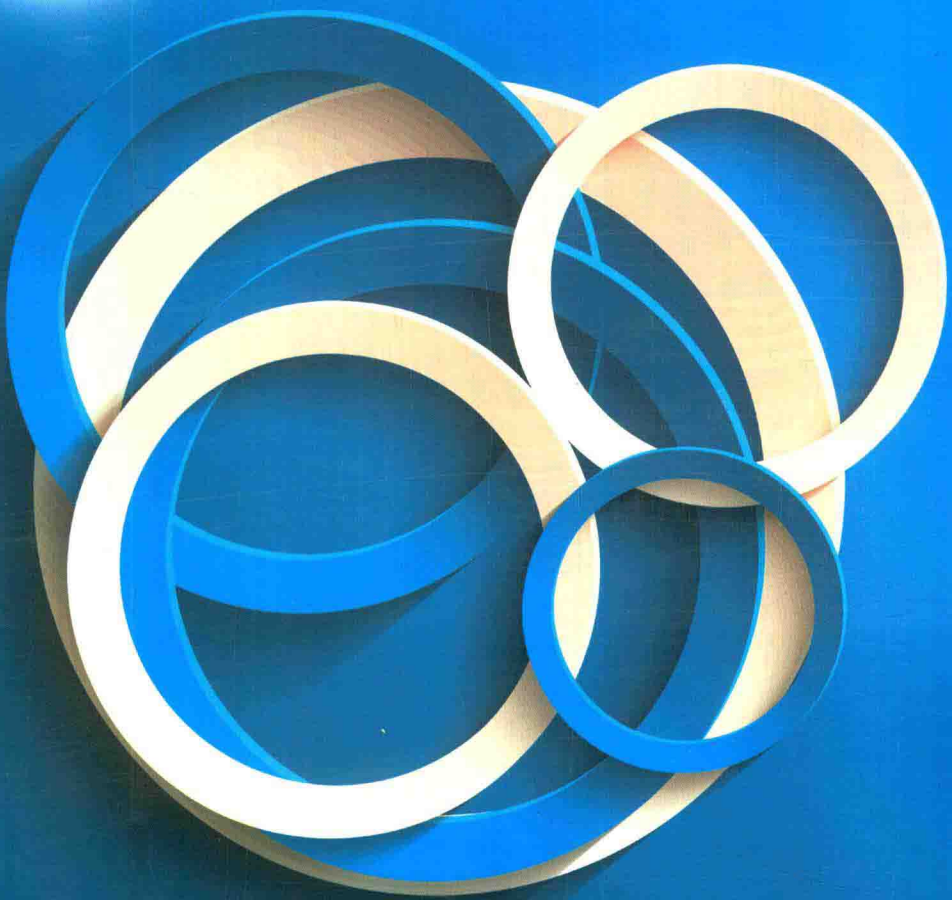
工业和信息产业科技与教育专著出版资金
cbji.phei.com.cn

基于岗位职业能力培养的
高职网络技术专业系列教材建设



网络安全基础及应用

李丹　主编

中国工信出版集团

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

工业和信息产业科技与教育专著出版资金资助出版
基于岗位职业能力培养的高职网络技术专业系列教材建设

网络安全基础及应用

李　丹　主　编
罗剑高　董兆殷　钟瑞琼　副主编
石　硕　主　审

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

本书以构建网络安全体系为主要框架，以网络安全主要技术为叙述脉络，以大量的实训和习题为支撑，全面地介绍了网络安全的基本概念、网络安全的体系结构，以及网络安全管理的各项内容和任务。全书共分为10章，内容涵盖了网络安全的基本概念、网络安全协议、密码技术、操作系统安全与管理、常用的网络攻击技术、恶意代码及防范技术、防火墙与入侵检测技术、IP安全与Web安全，最后通过一个真实的校园网安全案例使学生对网络安全方案的设计有一个全面和透彻的理解和掌握。

本书注重知识的实用性，以理论和实践相结合，选取大量的实训，使读者在系统地掌握网络安全技术的基础上，正确有效地解决网络安全领域中实际的问题。

图书在版编目（CIP）数据

网络安全基础及应用 / 李丹主编 . —北京 : 电子工业出版社，2016.1
基于岗位职业能力培养的高职网络技术专业系列教材建设

ISBN 978-7-121-27970-6

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

中国版本图书馆 CIP 数据核字（2015）第 317927 号

责任编辑：贺志洪
特约编辑：彭　瑛　罗树利
印　　刷：三河市鑫金马印装有限公司
装　　订：三河市鑫金马印装有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路173信箱　　邮编：100036
开　　本：787×1092　1/16　　印张：20　　字数：512千字
版　　次：2016年1月第1版
印　　次：2016年1月第1次印刷
印　　数：3000册　　定价：41.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至zlts@phei.com.cn，盗版侵权举报请发邮件至dbqq@phei.com.cn。

服务热线：（010）88258888。

编委会名单

编委会主任

吴教育	教授	阳江职业技术学院院长

编委会副主任

谢赞福	教授	广东技术师范学院计算机科学学院副院长
王世杰	教授	广州现代信息工程职业技术学院信息工程系主任

编委会执行主编

石　硕	教授	广东轻工职业技术学院计算机工程系
郭庚麒	教授	广东交通职业技术学院人事处处长

委员（排名不分先后）

王树勇	教授	广东水利电力职业技术学院教务处处长
张蒲生	教授	广东轻工职业技术学院计算机工程系
杨志伟	副教授	广东交通职业技术学院计算机工程学院院长
黄君羡	微软认证专家	广东交通职业技术学院计算机工程学院网络工程系主任
邹　月	副教授	广东科贸职业学院信息工程系主任
卢智勇	副教授	广东机电职业技术学院信息工程学院院长
卓志宏	副教授	阳江职业技术学院计算机工程系主任
龙　翔	副教授	湖北生物科技职业学院信息传媒学院院长
邹利华	副教授	东莞职业技术学院计算机工程系副主任
赵艳玲	副教授	珠海城市职业技术学院电子信息工程学院副院长
周　程	高级工程师	增城康大职业技术学院计算机系副主任
刘力铭	项目管理师	广州城市职业学院信息技术系副主任
田　钧	副教授	佛山职业技术学院电子信息系副主任
王跃胜	副教授	广东轻工职业技术学院计算机工程系
黄世旭	高级工程师	广州国为信息科技有限公司副总经理

秘书

贺志洪　电子工业出版社　hezhihongbnu@126.com

前言

Preface

more

随着计算机网络技术的飞速发展，信息网络已经成为社会发展的重要保证，信息网络涉及国家的政府、军事等诸多领域。存储、传输和处理的许多信息是政府的宏观调控决策、商业经济信息、银行资金转账、股票证券、能源资源数据、科研数据等重要信息，其中很多是敏感信息，甚至是国家机密，所以难免会吸引来自世界各地的各种人为的攻击。例如，信息泄露、信息窃取、数据篡改、数据增删、计算机病毒等。由此可见，网络安全是一个关乎国家安全和主权、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凸显，因此网络安全的学习及安全人才的培养越来越重要。

本书以网络安全技术基础知识为理论主线，同时结合大量实训作为学生的实践基础。全书共分为 10 章，前 4 章是网络安全的基本知识和技术的介绍，包含网络安全的基本概念，OSI 和 TCP/IP 参考模型中协议层的安全问题、密码技术，以及操作系统的安全与管理。第 5 章，通过讲述常用的网络攻击技术（这一章篇幅较多，也是读者最感兴趣的一章），通过黑客攻击的一般流程——踩点、扫描、攻击、种植后门、网络隐身，让读者掌握网络攻防的基本原理与方法。第 6 章，介绍当今流行的恶意代码的概念与类型，包括计算机木马病毒的原理与组成。第 7 章，重点讲解了网络安全的重要防御组件——防火墙和入侵检测系统，该部分可以使读者在网络安全体系构建中更好地运用防御技术保障网络的安全。第 8 章 IP 与 Web 安全，介绍了 IPSec 协议基本工作原理，以及 Web 安全领域中的 SSL/TLS 技术和 VPN 技术。第 9 章，通过一个实际的校园网安全案例，向读者展示了一个相对完整的网络安全方案的设计过程，从需求分析到方案实施，网络安全的技术得到了实际的应用与体现。最后在第 10 章中，对网络安全的发展和趋势进行了展望。

附录的 5 个教学实训项目，有难度并富有挑战性，更全面地考查学生的分析、解决问题的能力，教师可以根据学生的学习程度自行选择安排。

本书源于作者多年网络安全技术课程教学经验，以及对网络安全技术领域的探索，其主要特色包括如下几个方面：

- 知识点简洁、实用。
- 实验实训丰富，实验过程详细。
- 案例真实性和实用性较强。
- 习题资源丰富，知识面广，有针对性和扩展性。
- 附录给出了 5 个富有挑战性的实训项目。
- 为了帮助教师教学，我们提供了如下材料。
  - ➢ 习题答案。

- PPT幻灯片。
- 实验图表文件：本书的所有实验图和表的图片文件。

本书由广东轻工职业技术学院计算机系网络教研室李丹老师任主编，广东农工商职业技术学院计算机系副教授罗剑高老师、广东外语外贸大学信息学院副教授钟瑞琼老师、广东轻工职业技术学院网络中心董兆殷老师任副主编，也参与了编写工作。本书教学资源可以和出版社联系索取，或者发邮件到 lydia5280@163.com，联系李丹老师索取。

最后，感谢广东轻工职业技术学院计算机系石硕教授对本书技术方面的支持与帮助，感谢广东轻工职业技术学院网络中心的董兆殷老师提供的全面的校园网安全案例资源，感谢电子工业出版社束传政主任对于本书的编排给予的中肯、有价值的宝贵建议。

作　　者

2015 年 9 月

Contents

目录

more

第1章 网络安全概论

本章要点

- 网络安全的定义、基本要素和本质。
- 网络安全威胁的根源。
- 网络安全的防范。
- 网络安全的标准。
- 网络安全的法律法规。
- 黑客概述。

1.1 网络安全概述

网络空间已成为国家继陆、海、空、天四个疆域之后的第五疆域，与其他疆域一样，网络空间也须体现国家主权，保障网络空间安全也就是保障国家主权。党的十八大提出“要高度关注网络空间安全”，三中全会后成立了中央网络安全和信息化领导小组，这标志着我国网络空间安全国家战略已经确立。不久前习近平主席指出：“没有网络安全就没有国家安全，没有信息化就没有现代化。”这是在新的历史时期我国信息领域工作的指导方针。

中国互联网络信息中心（CNNIC）在2015年7月23日在京发布了第36次全国互联网发展统计报告。报告显示，上半年我国共新增网民1 894万人；截至2015年6月，互联网普及率为48.8%，我国网民总数已达6.68亿人。2015年中国网上零售额已接近两万亿元，电子商务正在逐步成为拉动消费的“主力军”，网络安全重要性日益凸显。PWC[①]发布的2015年全球信息安全状态调查报告指出，2014年，全球所有行业检测到的网络攻击共有4 280万次，比去年增长了48%。华盛顿战略和国际研究中心在2014年发布报告称，每年计算机及网络犯罪活动为世界经济带来的损失超过4 450亿美元。

上百万电脑黑客秘密潜伏伺机出动，在我们每天通过网络进行办公、学习、轻松买卖，享受方便的同时，也面临着窃听、信息篡改、病毒传播等多种网络安全威胁。面对互联网安全环境日益严峻趋势，数以万计的安全工作者守候在网民身边，坚持不懈地与网络犯罪战斗着，在移动、云、大数据日益改变生活的时代里，网络安全备受更大的考验。

① PWC：普华永道会计事务所

1.1.1 “网络安全”的由来

网络发展的早期，人们更多地强调网络的方便性和可用性，而忽略了网络的安全性。当网络仅仅用来传送一般性信息的时候，当网络的覆盖面积仅仅限于一幢大楼、一个校园的时候，安全问题并没有突出地表现出来。但是，当在网络上运行敏感性的业务如银行业务等，当企业的主要业务运行在网络上，当政府部门的活动正日益网络化的时候，计算机网络安全就成为一个不容忽视的问题。

如今，网络克服了地理上的限制，把分布在一个地区、一个国家，甚至全球的分支机构联系起来。它们使用公共的传输信道传递敏感的业务信息，通过一定的方式可以直接或间接地使用某个机构的私有网络。组织和部门的私有网络也因业务需要不可避免地与外部公众网直接或间接地联系起来，上述因素使得网络运行环境更加复杂，分布地域更加广泛，用途更加多样化，从而造成网络的可控制性急剧降低，安全性变差。

随着以计算机和网络通信为代表的信息技术（IT）的迅猛发展，现代政府部门、金融机构、军事军工、企事业单位和商业组织对 IT 系统的依赖也日益加重，信息技术几乎渗透到了世界各地和社会生活的方方面面。正是因为组织机构的正常运转高度依赖 IT 系统，IT 系统所承载的信息和服务的安全性就越发显得重要。

组织和部门对网络依赖性增强，一个相对较小的网络也突出地表现出一定的安全问题，尤其是当组织的部门的网络就要面对来自外部网络的各种安全威胁，即使是网络自身利益没有明确的安全要求，也可能由于被攻击者利用而带来不必要的法律纠纷。网络黑客的攻击、网络病毒的泛滥和各种网络业务的安全要求已经构成了对网络安全的迫切需求。

“计算机网络安全”，尽管现在这个词很火，但是真正对它有正确认识的人不多。要正确定义计算机网络安全并不容易，困难在于要形成一个足够全面而有效的定义。通常来讲，安全就是“避免冒险和危险”。在计算机科学当中，安全就是防止未授权的使用者访问信息，以及未授权而试图破坏或更改信息，这可以重述为“安全就是一个保护系统信息和系统资源相应的机密性和完整性的能力”。

1.1.2 网络安全的定义

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。是指网络系统的硬件、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受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

网络安全的具体含义会随着“角度”的变化而变化。比如：从用户（个人、企业等）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，避免其他人或对手利用窃听、冒充、篡改、抵赖等手段侵犯用户的利益和隐私。

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，以及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，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。

1.1.3 网络安全的基本要素

网络安全从其本质上来讲就是网络上的信息安全。从广义来说，凡是涉及网络上信息的机密性、完整性、可用性、可控性和可审查性的相关技术和理论都是网络安全的研究领域。

所以网络安全应具有如下五个方面的特征。

- 机密性：信息不泄露给非授权用户、实体或过程，或供其利用的特性。
- 完整性：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。
- 可用性：可被授权实体访问并按需求使用的特性。即攻击者不能占用所有资源而阻碍授权者工作。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。
- 可控性：可以控制授权范围内的信息流向和行为方式。
- 可审查性：对出现的安全问题提供调查的依据与手段。

其中的机密性（Confidentiality）、完整性（Integrity）、可用性（Availability）是网络信息安全的三个最基本的目标，简称 CIA 三元组。

1.2 网络安全威胁的根源

1.2.1 物理安全问题

网络的物理安全是整个网络系统安全的前提。在网络信息系统建设中，由于网络系统属于弱电工程，耐压值很低。因此，在网络工程的设计和施工中，必须优先考虑保护人和网络设备不受电、火灾和雷击的侵害；需要考虑布线系统与照明电线、动力电线、通信线路、暖气管道及冷热空气管道之间的距离；考虑布线系统和绝缘线、裸体线，以及接地与焊接的安全；必须建设防雷系统，防雷系统不仅考虑建筑物防雷，还必须考虑计算机及其他弱电耐压设备的防雷、水灾、火灾等环境事故；电源故障；人为操作失误或错误；设备被盗、被毁；电磁干扰；线路截获；高可用的硬件；双机多冗余设计；机房环境及报警系统、安全意识等。因此尽量避免网络的物理安全风险。

除物理设备本身的问题外，物理安全问题还包括设备的位置安全、限制物理访问、物理环境安全和地域因素等。物理设备的位置极为重要。所有基础网络设施都应该放置在严格限制来访人员的地方，以降低出现未经授权访问的可能性。

1.2.2 方案设计缺陷

由于在实际中，网络的结构往往比较复杂，为了实现异构网络间信息的通信，往往要牺

牲一些安全机制的设置和实现，从而提出更高的网络开放性的要求。开放性和安全性正是一对相生相克的矛盾。

由于特定的环境往往会有特定的安全需求，所以不存在可以到处通用的解决方案，往往需要制订不同的方案。如果设计者的安全理论与实践水平不够，设计出来的方案经常会出现很多漏洞，这也是安全威胁的根源之一。

1.2.3 系统安全漏洞

随着软件规模的不断增大，系统中安全漏洞或后门也不可避免地存在，比如我们常用的操作系统，无论 Windows 还是 Linux 几乎都或多或少地存在安全漏洞，诸多各类服务器中最典型的如微软的 IIS 服务器、浏览器、数据库等都被发现存在安全隐患。可以说任何一个软件系统都可能因为程序员的一个疏忽、设计中一个缺陷等原因而存在安全漏洞，这也是网络安全问题的主要根源之一。

目前我们发现的安全漏洞数量已经相当庞大，据统计已经接近病毒的数量，如下列举了了一些典型的安全漏洞。它们在新发布的系统或已经打过补丁的系统中可能已经不再存在，但是了解它们依然具有非常积极的意义。

1）操作系统类安全漏洞

操作系统中的安全漏洞包括非法文件访问、远程获得 ROOT 权限、系统后门、NIS 漏洞、FINGER 漏洞、RPC 漏洞等。

2）网络系统类安全漏洞

典型例子包括，CISCO IOS 的早期版本不能抵抗很多拒绝服务类的攻击（如 LAND）。

3）应用系统类安全漏洞

各种应用都可能隐含安全缺陷，尤其是较早的一些产品和国内的一些公司的产品对安全问题很少考虑，如通过 TCP/IP 协议应用 Mail Server、WWW Server、FTP Server、DNS 时出现的安全漏洞等。

1.2.4 TCP/IP协议的安全问题

因特网最初设计考虑是该网不会因局部故障而影响信息的传输，基本没有考虑安全问题，因此在安全可靠与服务质量、带宽和方便性等方面存在一些矛盾。作为因特网灵魂的 TCP/IP 协议，更存在很大的安全隐患，缺乏强健的安全机制，这也是网络不安全的主要因素之一。

下面以 TCP/IP 的主要协议——IP 协议作为例子来说明这个问题。

IP 协议依据 IP 头中的目的地址项来发送 IP 数据包，如果目的地址是本地网络内的地址，该 IP 包被直接发送到目的地址；如果目的地址不在本地网络内，该 IP 包就被发送到网关，再由网关决定将其发送到何处，这是 IP 协议路由 IP 包的方法。