工业和信息化普通高等教育“十二五”规划教材立项项目
21世纪高等院校网络工程规划教材
21st Century University Planned Textbooks of Network Engineering

网络安全实用教程

Network Security

刘远生 主编
李剑勇 李康乐 副主编

- 重点介绍网络安全技术及其应
- 配以丰富的应用实例和实践内
- 培养学生网络管理、安全技术应用能力和实践操作技能

人民邮电出版社
POSTS & TELECOM PRESS

工业和信息化普通高等教育“十二五”规划教材立项项目
21世纪高等院校网络工程规划教材
21st Century University Planned Textbooks of Network Engineering

网络安全实用教程

刘远生 主编
李剑勇 李康乐 副主编

人 民 邮 电 出 版 社
北 京

图书在版编目（CIP）数据

网络安全实用教程 / 刘远生主编. -- 北京 : 人民邮电出版社, 2011.4
21世纪高等院校网络工程规划教材
ISBN 978-7-115-24887-9

Ⅰ. ①网… Ⅱ. ①刘… 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(2011)第031678号

内 容 提 要

本书介绍了计算机网络安全的基本知识、安全技术和应用实践。主要内容可分为三大部分：第一部分为网络安全基础，主要介绍了网络安全的基本知识、安全风险和安全威胁、OSI 安全体系结构等；第二部分介绍了网络安全涉及的各种安全技术，如密码技术、防火墙、安全认证、EFS、IPSec、黑客攻击及防范、漏洞扫描、网络监听、入侵检测、病毒防治等；第三部分为网络安全应用实践，主要介绍了一些比较重要的网络产品（如路由器、交换机、服务器、VPN 及软件工具）的安全配置及其技术应用。

本书内容丰富，概念清楚，语言精练，通俗易懂，理论联系实际，易于教学。本书可作为高等院校计算机、通信和信息安全等专业的教材，也可以作为网络安全工程师、网络管理员和计算机用户的参考用书，以及网络安全培训教材。

21 世纪高等院校网络工程规划教材

网络安全实用教程

◆ 主　　编　刘远生
副 主 编　李剑勇　李康乐
责任编辑　刘　博

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
邮编　100061　　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
中国铁道出版社印刷厂印刷

◆ 开本：787×1092　1/16
印张：19.25　　2011 年 4 月第 1 版
字数：483 千字　　2011 年 4 月北京第 1 次印刷

ISBN 978-7-115-24887-9

定价：34.00 元

读者服务热线：(010)67170985　印装质量热线：(010)67129223
反盗版热线：(010)67171154

前　言

随着 Internet 的迅猛发展，计算机网络已成为人类社会的重要组成部分，无论在经济、政治和军事领域，还是在人们的交流、工作和学习中，都发挥着越来越重要的作用。因此，计算机网络也自然成为人类竞争和冲突的手段与目标，这是计算机网络面临安全威胁和需要加强安全防护的根本原因。网络安全，尤其是 Internet 安全正面临着严重的挑战。一方面是 Internet 规模的扩大和应用服务的激增，导致人们对网络安全的需求提高；另一方面黑客入侵、病毒传播以及形形色色的网络攻击日益增加，网络安全防线十分脆弱，使实施网络安全的难度大大增加。

频繁发生的网络病毒破坏、黑客入侵窃密和网络金融犯罪等活动，使人们深刻意识到了网络安全威胁的严重性和安全防护的迫切性，同时网络安全已经成为关系个人与社会生活的重大问题，也同样成为一个亟待解决而又十分复杂的课题。解决网络安全问题更多地涉及网络安全技术、网络系统管理和实际应用。每一位网络管理人员、网络系统用户和工程技术人员都应该了解和掌握一定的网络安全知识和技术，以便使自己的信息系统能够安全、稳定地运行，并提供正常的服务。

目前关于网络安全的教材和参考书已很多，但一般都是理论知识和技术原理介绍得较多，网络软件工具应用、系统安全案例和实际操作介绍得较少，较适合于研究型大学的本科生或研究生使用。而对于应用型本科和高职高专学生而言，在了解简单的网络安全知识和技术原理的基础上，应重点掌握和熟练运用相关的网络安全技术解决实际问题。

本书按照应用型本科人才的培养目标和要求，以网络信息安全和网络安全应用能力的培养为主导，介绍了网络安全的基本知识和技术；在体系结构和内容上进行了有益的探索，既保持了一定的知识系统性，又使各章内容具有一定的独立性；使教学内容与专业、行业的应用及人才培养相适应。本书的主要内容可分为三大部分：第一部分为网络安全基础，主要介绍了网络安全的基本知识、安全风险、安全威胁和 OSI 安全体系结构等；第二部分介绍了网络安全涉及的各种安全技术，如密码技术、防火墙、安全认证、EFS、IPSec、黑客攻击及防范、漏洞扫描、网络监听、入侵检测、病毒防治等；第三部分为网络安全应用实践，主要介绍了一些比较重要的网络产品（如路由器、交换机、服务器、VPN 及软件工具）的安全配置及其技术应用。全书共分为 10 章，内容包括网络安全概述、网络操作系统安全、网络数据库安全、网络硬件设备安全、网络软件安全、数据加密与认证技术、网络病毒及其防治、网络的攻击与防护、无线网络安全与应用和 Internet 安全与应用。

本书本着理论知识必需、够用的原则，在简捷介绍理论知识的基础上重点介绍网络安全技术的应用，并结合目前网络安全技术在社会乃至家庭中的实际应用，将近年来出现的实用技术及新型工具软件融入教材中。本书典型实例的应用性和可操作性强，着重网络安全的应用技术、案例及其操作技能的知识介绍，培养学生的理论联系实际能力、网络应用能力和网络实际应用技能。通过本书的学习，可使读者较好地了解和掌握计算机网络安全方面的基础知识和实用技术，掌握实际网络安全管理、安全技术和信息安全保护的应用能力。

本书内容丰富，概念清楚，语言精练，通俗易懂，理论联系实际，易于教学；章末配有

习题，便于学生学习和实践。为了方便师生的教与学，该教材配有 PPT 电子教案，并附有实用网络设备的模拟器安全配置程序。电子教案和设备配置模拟器程序可从人民邮电出版社教学服务与资源网（www.ptpedu.com.cn）上免费下载。本书可作为高等院校计算机专业、通信专业及相关专业学生的教材，也可以作为网络安全工程师、网络管理员和计算机用户的参考用书，或作为网络安全培训教材。

本书由刘远生任主编，李剑勇、李康乐任副主编，李民、李荣霞、牟瑛、庞德彬和张伟参加了编写，全书由刘远生统阅定稿。

由于网络安全涉及的技术领域较广，且编写的时间较紧，因此书中难免存在错误或叙述不当之处，欢迎广大读者提出宝贵意见，并恳请各位专家、学者给予批评指正。编者也希望与读者多交流，联系方式为 ysliu@sjtu.edu.cn。

编　者

2011 年 1 月

目　录

第 1 章　网络安全概述

随着计算机网络技术的迅速发展和普及应用，人类已进入数字化、网络化和信息化时代，计算机网络技术的发展与应用已成为影响一个国家和地区政治、经济、军事、科学与文化发展的重要因素之一。但由于计算机网络具有开放性和互连性等特征，致使网络易受黑客和病毒的攻击和入侵，使网络系统遭到破坏，导致信息的泄露或丢失。因此，如何有效地保证网络安全，已成为人们非常关注的问题。

本章主要介绍网络安全的概念、网络安全的威胁与风险管理、网络安全体系、网络安全策略与技术、网络安全级别和网络系统安全的日常管理等内容。

1.1　网络安全概论

网络安全是一门涉及领域相当广泛的学科，这是因为在目前的公用通信网络中存在着各种各样的安全漏洞和威胁。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。

1.1.1　网络安全的概念

网络安全本质上就是网络上的信息系统安全。网络安全包括信息系统的安全运行和系统信息的安全保护两方面。信息系统的安全运行是信息系统提供有效服务（即可用性）的前提，系统信息的安全保护主要是确保数据信息的机密性和完整性。

从不同的角度来看，网络安全又具有不同的含义。

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能够受到机密性、完整性和真实性的保护，避免其他人或竞争对手利用窃听、冒充、篡改或抵赖等手段对用户的利益和隐私造成损害，同时也希望当信息保存在某个计算机系统上时，不受其他非法用户的非授权访问和破坏。

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读写等操作受到保护和控制，避免出现病毒、非法存取、拒绝服务或网络资源的非法占用及非法控制等威胁，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，避免其通过网络泄露，避免由于这类信息的泄密对社会产生危害，给国家造成巨大的经济损失，甚至威胁到国家安全。

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产

生不良影响，必须对其进行控制。

由此可见，网络安全在不同的环境和具体的应用中可以有不同的解释。

1.1.2 网络安全的需求与目标

网络安全的目标主要表现在系统的可用性、可靠性、机密性、完整性、不可抵赖性及可控性等方面。

1. 可用性

可用性是网络信息可被授权实体访问并按需求使用的特性。由于网络最基本的功能就是为用户提供信息和通信服务，而用户对信息和通信的需求是随机的（内容的随机性和时间的随机性）、多方面的（文字、语音、图像等），有的用户还对服务的实时性有较高的要求。网络必须能保证所有用户的通信需要，一个授权用户无论何时提出要求，网络都必须是可用的，不能拒绝用户的要求。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。对于此类攻击，一方面要采取物理加固技术，保障物理设备安全可靠地工作；另一方面要通过访问控制机制，阻止非法用户进入网络。

2. 可靠性

可靠性是指网络信息系统能够在规定条件下，在规定时间内，实现规定功能的特性。可靠性是网络安全最基本的要求之一，是所有网络信息系统建设和运行的目标。目前，对于网络可靠性的研究偏重于硬件方面，主要采用硬件冗余、提高可靠性和精确度等方法提高网络可靠性。实际上，软件的可靠性、人员的可靠性和环境的可靠性在保证系统可靠性方面也是非常重要的。

3. 机密性

机密性是网络信息不被泄露给非授权用户、实体或过程，或为其利用的特性。这些信息不仅指国家机密，也包括企业和社会团体的商业和工作秘密，还包括个人的秘密（如银行账号）和个人隐私等。机密性主要通过信息加密、身份认证、访问控制、安全通信协议等技术实现，它是在可用性和可靠性的基础上，保障网络信息安全的重要手段。

4. 完整性

完整性是网络信息未经授权不能进行改变的特性。网络信息在存储或传输过程中应保证不被偶然或蓄意地篡改或伪造，保证授权用户得到的信息是真实的。如果信息被未经授权的实体修改了或在传输过程中出现了错误，信息的使用者应能够通过一定的方式判断出信息是否真实可靠。

5. 不可抵赖性

不可抵赖性也称为可审查性，是指通信双方在通信过程中，对自己所发送或接收的消息不可抵赖，即发送者不能否认他发送过消息的事实和消息的内容，接收者也不能否认其接收到消息的事实和消息的内容。

6. 可控性

可控性是对网络信息的内容及其传播具有控制能力的特性。保障系统依据授权提供服

务，使系统在任何时候都不被非授权人使用，对黑客入侵、口令攻击、用户权限非法提升、资源非法使用等采取防范措施。

1.2　网络安全的威胁与风险管理

网络的开放性和共享性在方便人们的同时，也使得网络系统容易受到黑客攻击。网络的安全威胁是指对网络系统的网络服务、网络信息的机密性和可用性产生不利影响的各种因素。网络的安全威胁中也包括缓冲区溢出、假冒用户、电子欺骗等安全漏洞。

1.2.1　网络系统漏洞

目前，没有安全漏洞的计算机网络几乎是不存在的。而正是这些漏洞使得攻击能够成功，从而引起了攻击者的兴趣。安全漏洞是网络攻击的客观原因，它与许多技术因素有关。

1. 漏洞的概念

从广义上讲，漏洞是在硬件、软件、协议的具体实现或系统安全策略以及人为因素上存在的缺陷，从而可以使攻击者能够在未经系统合法用户授权的情况下访问或破坏系统。全世界的路由器、服务器、客户端软件、操作系统和防火墙等每时每刻都会有很多漏洞出现，它们会影响到很大范围内的网络安全。

漏洞是由于系统设计人员、制造人员、检测人员或管理人员的疏忽或过错而隐藏在系统中的。发现漏洞的人主要包括计算机专家、黑客、安全服务商、安全组织、系统管理员和个人用户等。当发现漏洞时，计算机专家和安全服务商组织通常会向安全组织机构发出警告。黑客发现新漏洞后会采用新的攻击方法进行网络攻击，新的攻击方法意味着新漏洞的发现，因此黑客是通过网络攻击活动间接发布漏洞信息的。

1988 年美国的莫里斯蠕虫事件，导致上千台计算机崩溃，造成了巨大的损失。该事件使人们认识到网络安全状况的脆弱性和突发性，以及对网络安全事件进行紧急响应的重要性。在美国国防部资助下，卡内基梅隆大学软件工程研究中心成立了世界上第一个计算机紧急响应小组（Computer Emergency Response Team，CERT）。20 余年来，CERT 在反击大规模的网络入侵方面起到了重要作用。CERT 是著名的信息安全组织，专门处理计算机网络安全问题。CERT 主要提供针对新的安全漏洞发布建议；24 小时全天候为遭受破坏的用户提供重要技术意见；利用它的 Web 站点提供有用的安全信息等服务。

2. 漏洞类型

根据漏洞的载体（网络实体）类型，漏洞主要分为操作系统漏洞、网络协议漏洞、数据库漏洞和网络服务漏洞等。

（1）操作系统漏洞

任何操作系统都可能存在漏洞，这些漏洞产生的原因很多，主要有以下几种。

① 操作系统陷门。一些操作系统为了安装其他公司的软件包而保留了一种特殊的管理程序功能，尽管此功能的调用需要以特权方式进行，但如果未受到严密的监控和必要的认证限制，就有可能形成操作系统陷门。

② 输入输出的非法访问。有些操作系统一旦 I/O 操作被检查通过后，该操作系统就默认继续执行而不再进行检查，从而造成后续操作的非法访问。还有些操作系统使用公共系统缓冲区，任何用户都可以搜索该缓冲区，如果该缓冲区没有严格的安全措施，那么其中的机密信息（如用户的认证数据、口令等）就有可能被泄露。

③ 访问控制的混乱。在操作系统中，安全访问强调隔离和保护措施，而资源共享要求开放。如果在设计操作系统时不能处理好这二者之间的矛盾关系，就可能出现安全问题。

④ 不完全的中介。完全的中介必须检查每次访问请求以进行适当的审批。而某些操作系统省略了必要的安全保护。要建立安全的操作系统，必须构造操作系统的安全模型并提供不同的实施方法。另外，还需要建立和完善操作系统的评估标准、评价方法和测试质量。

（2）网络协议漏洞

TCP/IP 的目标是保证通信和传输。TCP/IP 没有提供内在的控制机制支持源地址的鉴别，这是 TCP/IP 漏洞的根本原因。黑客会利用 TCP/IP 的这个漏洞，使用侦听方法来获取数据，进而对数据进行检查、推测 TCP 的序列号、修改传输路由、修改鉴别过程、插入黑客指令等。

（3）数据库漏洞

数据库管理系统（DBMS）作为操作系统的应用程序，其库文件可以看作是操作系统上的一个客体，其应用进程又是操作系统的主体。因此，数据库的安全是以操作系统的安全为基础的，没有操作系统的安全，就谈不上数据库的安全。但是，并不是有了安全的操作系统，就能绝对保证数据库的安全。由于对数据库的管理是建立在分级管理的概念上的，所以，其安全性是可想而知的。

（4）网络服务漏洞

① 匿名 FTP。匿名 FTP 是人们常用的一种 FTP 服务方式。多数 FTP 服务器可以用“Anonymous”用户名登录，这样就存在用户破坏系统和文件的可能性。另外，上传的软件可能具有破坏性，大量上传的文件还会耗费磁盘空间。建立匿名服务器时，应当确保用户不能访问系统的重要部分，尤其是包含系统配置信息的文件目录。如果没必要使用匿名登录，应将其关闭，并定时检查服务器日志。

② 电子邮件。电子邮件服务器本身就存在安全漏洞，一旦漏洞被黑客利用就可能对网络造成巨大的威胁。如 UNIX/Linux 系统的邮件服务器 Sendmail 是以“root”账号运行的，如果黑客掌握了这个漏洞就可以利用它来攻击系统。已经有蠕虫病毒利用 Sendmail 的安全缺陷使大批的网络服务器陷于瘫痪的案例。

③ 域名服务（DNS）。DNS 需要用户提供用户机器的硬件和软件信息。黑客经常把它作为一种攻击目标。假冒的 DNS 服务器可能会提供一些错误的信息甚至错误的域名解析，这样就造成了 DNS 欺骗。

④ Web 服务。Web 服务器本身存在漏洞，如 IIS（运行于 Windows 下）和 Apache（运行于 UNIX 下）本身的漏洞，使得黑客能入侵到主机系统，破坏一些重要数据，甚至造成系统瘫痪。另外，程序员在编写 CGI 程序时会预留一些“bug”，从而为网络攻击者创造了条件。

3. 典型的网络结构及安全漏洞

典型的网络结构及安全漏洞如图 1.1 所示，这些安全漏洞及其原因如下。

（1）不充分的路由器访问控制。配置不当的路由器 ACL 会使 ICMP、IP 和 NetBIOS 信息泄露，从而导致对目标网点 DMZ 上服务器所提供的服务进行未授权的访问。

（2）未实施安全措施且无人监管的远程访问网点，容易成为攻击者进入网络的入口。

（3）操作系统和应用程序、用户或用户组、共享资源、DNS 信息以及运行中的服务（如 SNMP）等信息不经意地泄露给攻击者。

（4）运行非必要服务（如 FTP 等）的主机提供了进入内部网络的通道。

（5）客户机上级别低的、易于被猜中或重用的口令使服务器易被入侵。

（6）具有过多特权的用户账号或测试账号。

（7）配置不当的 Internet 服务器，特别是 Web 服务器上 CGI 脚本和匿名 FTP。

（8）配置不当的防火墙或路由器导致直接侵入某个服务器后访问内部系统。

（9）没有打过补丁的、过时的、脆弱的或仍采用默认配置状态的软件。

（10）过度的文件和目录访问控制。

（11）过度的信任关系给攻击者提供未授权访问敏感信息的机会。

（12）不加认证的服务。

（13）没有采纳公认的安全策略、规程、指导和最低基线标准。

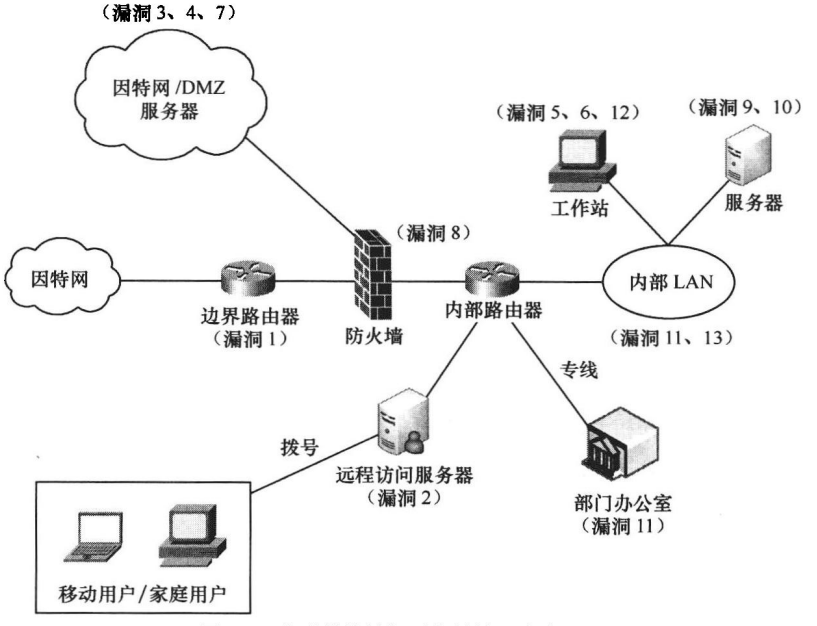

图 1.1　典型的计算机网络结构及安全漏洞

1.2.2　网络系统威胁

网络的安全威胁来自于网络中存在的不安全因素。网络不安全因素有两方面，一方面是网络本身的不可靠性和脆弱性；另一方面是人为破坏，这也是网络信息安全的最大威胁。网络安全的主要威胁有以下几种。

1. 物理威胁

物理威胁在网络中是最难控制的，它可能来源于外界的有意或无意的破坏。物理威胁有时可以造成致命的系统破坏。因此，防范物理威胁是很重要的。但在网络管理和维护中很多物理威胁往往被忽略，如网络设备被盗等。另外，在更换设备时，注意销毁无用系统信息也

很重要。如在更换磁盘时，必须对不用的磁盘进行格式化处理，因为利用反删除软件很容易恢复仅从磁盘上删除的文件。

2. 操作系统缺陷

操作系统是用户在使用计算机前必须安装的系统软件。很多操作系统在安装时都存在端口开放、无认证服务和初始化配置等问题，而这些又是操作系统自带的系统应用程序，如果这些应用程序有安全缺陷，那么系统就会处于不安全状态，这将极大地影响系统的信息安全。

3. 网络协议缺陷

由于 TCP/IP 在最初设计时并没有把安全作为重点考虑，而所有的应用协议都是基于 TCP/IP 的，因此各种网络底层协议本身的缺陷将会极大地影响上层应用的安全。

4. 体系结构缺陷

在现实应用中，大多数体系结构的设计和实现都存在着安全问题，即使是完美的安全体系结构，也有可能会因为一个小小的编程缺陷而被攻击。另外，安全体系中的各种构件如果缺乏密切的合作，也容易导致整个系统被各个击破。

5. 黑客程序

黑客（Hacker）的原意是指具有高超编程技术、强烈解决问题和克服限制欲望的人，而现在泛指那些强行闯入系统或以某种恶意的目的破坏系统的人。黑客程序是一类专门用于通过网络对远程计算机设备进行攻击，进而控制、窃取、破坏信息的软件程序。

6. 计算机病毒

计算机病毒是指在计算机程序中编制或插入的、破坏计算机功能或数据的、影响计算机使用且能够自我复制的一组计算机指令或程序代码，它具有寄生性、潜伏性、传染性和破坏性等特征。随着网络技术的发展，计算机病毒的种类越来越多，如系统病毒、脚本病毒、宏病毒、后门病毒和捆绑机病毒等。

1.2.3 网络安全的风险评估

由于网络系统会受到多种形式的威胁，所以绝对安全与可靠的网络系统是不存在的，只能通过一定的措施把风险降到一个可以接受的程度。定期地对企业的安全工作进行分析是非常重要的，但同样不可轻视的还包括在这个过程中进行网络风险评估。

风险评估（Risk Assessment）是对信息资产面临的威胁、存在的弱点、造成的影响，以及三者综合作用而带来风险的可能性的评估。作为风险管理的基础，风险评估是确定信息安全需求的一个重要途径，属于组织信息安全管理体系规划的过程。

网络安全的风险评估是有效保证信息系统安全的前提条件。只有准确地了解系统的安全需求、安全漏洞及其可能的危害，才能制定并实施正确的安全策略。另外，风险评估也是制定安全管理措施的依据之一。网络风险评估包括对来自企业外部的网络风险和企业内部的网络风险进行评估。对企业内部的网络风险评估与外部的风险评估使用相同的方法，不过要从

访问内网的用户角度来指导进行。

通过对网络系统全面、充分、有效的安全评估，能够快速检测出网络上存在的安全隐患、网络系统中存在的安全漏洞、网络系统的抗攻击能力等。根据对网络业务的安全需求、安全策略和安全目标的评估结果，可以提出合理的安全防护措施建议。网络安全评估主要有以下项目。

- 安全策略评估。
- 网络物理安全评估。
- 网络隔离的安全性评估。
- 系统配置的安全性评估。
- 网络防护能力评估。
- 网络服务的安全性评估。
- 网络应用系统的安全性评估。
- 病毒防护系统的安全性评估。
- 数据备份的安全性评估。

网络安全在过去一直倾向于采取被动式管理的防护策略，被动式防护所使用的设备及工具也是最省事且直接有效的，例如防火墙、入侵检测等。但在复合式病毒出现后，被动式防护策略已显得防御力不足。漏洞扫描仪是网络安全中评估弱点及风险的重要工具，其主要功能是找出网络主机及设备的漏洞、隐藏性风险以及鉴定网络架构的安全程度。漏洞扫描仪可对 SMTP、POP、HTTP、FTP、SNMP、Telnet、SSH、NFS 等协议和账号密码管理疏失及不当的设定进行安全检测，还可对防火墙、路由器等硬设备以及数据库服务器等进行检测。漏洞扫描后所产生的风险评估安全报告可分别提供给管理者及技术人员，管理者报告仅提供整个网络的安全状态及风险程度分析，而技术人员报告则提供每一个弱点说明、修补建议和修补方法。这样可将隐藏性风险及威胁降至最低，使原本必需大费周折的弱点安全评估工作变得轻松容易。

一般来说，一个有效的网络风险评估方法可以解决以下问题。

- 防火墙配置不当的外部网络拓扑结构。
- 路由器过滤规则的设置不当。
- 弱认证机制。
- 配置不当或易受攻击的电子邮件和 DNS 服务器。
- 潜在的网络层 Web 服务器漏洞。
- 配置不当的数据库服务器。
- 易受攻击的 FTP 服务器。

1.3　网络安全体系

网络安全体系结构是网络安全层次的抽象描述。在大规模的网络工程建设、管理及基于网络安全系统的设计与开发过程中，需要从全局的体系结构角度考虑安全问题的整体解决方案，才能保证网络安全功能的完备性和一致性，降低安全代价和管理开销。这样的网络安全体系结构对于网络安全的设计、实现与管理都有重要的意义。

网络安全是一个范围较广的研究领域，人们一般都只是在该领域中的一个小范围做自己的研究，提出能够解决某种特殊的网络安全问题的方案。比如，有人专门研究加密和鉴别，有人

专门研究入侵和检测，有人专门研究黑客攻击等。网络安全体系结构是一种从系统化的角度理解这些安全问题的解决方案，对研究、实现和管理网络安全的工作具有全局性指导作用。

1.3.1 OSI 安全体系

1. OSI 参考模型

OSI 参考模型是国际标准化组织（ISO）为解决异种机互连而制定的开放式计算机网络层次结构模型，它的最大优点是将服务、接口和协议这三个概念明确地区分开来。OSI 参考模型将计算机网络划分为七个层次，自下而上分别称为物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。

ISO 于 1989 年 2 月公布的 ISO7498-2“网络安全体系结构”文件，给出了 OSI 参考模型的安全体系结构，简称 OSI 安全体系结构。这是一个普遍适用的安全体系结构，它对具体网络的安全体系结构具有指导意义，其核心内容是保证异构网络系统之间远距离交换信息的安全。

OSI 安全体系结构主要包括网络安全机制和网络安全服务两方面的内容。网络安全机制和网络安全服务与 OSI 网络层次之间形成了一定的逻辑关系。

2. 网络安全机制

在“网络安全体系结构”文件中规定的网络安全机制有 8 项：加密机制、数字签名机制、访问控制机制、数据完整性机制、交换鉴别机制、信息量填充机制、路由控制机制和公证机制。OSI 网络安全体系结构、OSI 安全服务，以及 OSI 安全服务与安全机制之间的关系分别见图 1.2、表 1.1 和表 1.2。

（1）加密机制

数据加密是提供信息保密的主要方法，可保证数据存储和传输的保密性。此外，加密技术与其他技术结合，可保证数据的完整性。

（2）数字签名机制

数字签名可解决传统手工签名中存在的安全缺陷，在电子商务中使用较广泛。数字签名主要解决否认问题（发送方否认发送了信息）、伪造问题（某方伪造了文件却不承认）、冒充问题（冒充合法用户在网上发送文件）和篡改问题（接收方私自篡改文件内容）。

（3）访问控制机制

访问控制机制可以控制哪些用户对哪些资源可以进行访问，对这些资源可以访问到什么程度。如非法用户企图访问资源，该机制则会加以拒绝，并将这一非法事件记录在审计报告中。访问控制可以直接支持数据的保密性、完整性和可用性，它对数据的保密性、完整性和可用性所起的作用是非常明显的。

（4）数据完整性机制

数据完整性机制保护网络系统中存储和传输的软件（程序）和数据不被非法改变，如添加、删除、修改等。

（5）交换鉴别机制

交换鉴别机制是通过相互交换信息来确定彼此的身份。在计算机中，鉴别主要有站点鉴别、报文鉴别、用户和进程的认证等，通常采用口令、密码技术、实体的特征或所有权等手

段进行鉴别。

（6）信息量填充机制

攻击者可能会对传输信息的长度、频率等特征进行统计，以便进行信息流量分析，从中获得有用的信息。采用信息量填充机制，可保持系统信息量基本恒定，因此能防止攻击者对系统进行信息流量分析。

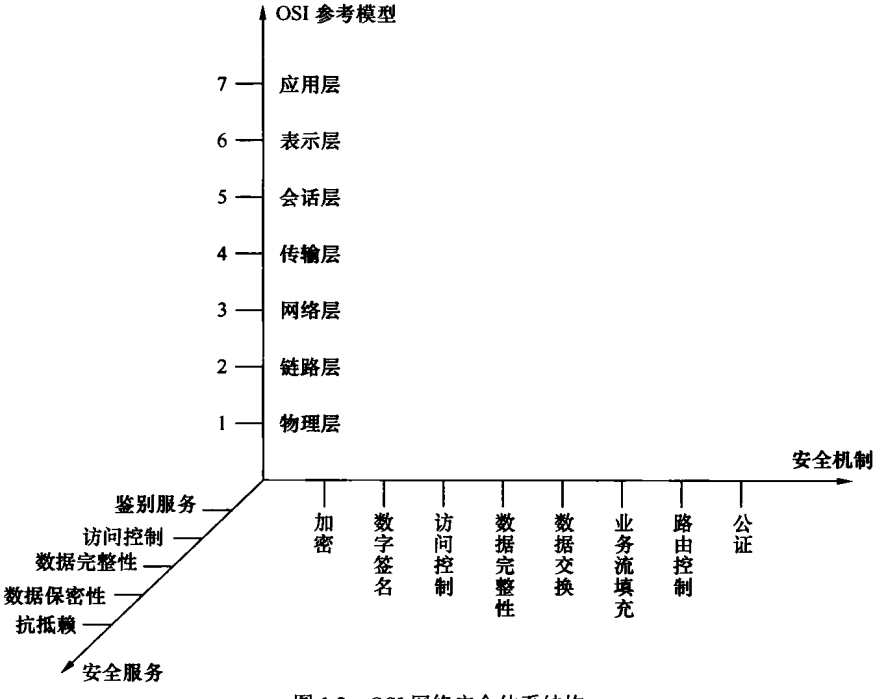

图 1.2　OSI 网络安全体系结构

（7）路由控制机制

路由控制机制可以指定通过网络发送数据的路径，因此，采用该机制可以选择那些可信度高的节点传输信息。

（8）公证机制

公证机制就是在网络中设立一个公证机构，来中转各方交换的信息，并从中提取相关证据，以便对可能发生的纠纷做出仲裁。

3. 网络安全服务

在“网络安全体系结构”文件中规定的网络安全服务有 5 项：鉴别服务、访问控制服务、数据完整性服务、数据保密性服务和非否认服务。

（1）鉴别服务

鉴别服务包括同等实体鉴别和数据源鉴别两种服务。使用同等实体鉴别服务可以对两个同等实体（用户或进程）在建立连接和开始传输数据时进行身份的合法性和真实性验证，以防止非法用户的假冒，也可防止非法用户伪造连接初始化攻击。数据源鉴别服务可对信息源点进行鉴别，可确保数据是由合法用户发出的，以防假冒。

（2）访问控制服务

访问控制包括身份验证和权限验证。访问控制服务防止未授权用户非法访问网络资源，

也防止合法用户越权访问网络资源。

（3）数据完整性服务

数据完整性服务防止非法用户对正常数据的变更，如修改、插入、延时或删除，以及在数据交换过程中的数据丢失。数据完整性服务可分为以下 5 种情形，通过这些服务来满足不同用户、不同场合对数据完整性的要求。

- 带恢复功能的面向连接的数据完整性。
- 不带恢复功能的面向连接的数据完整性。
- 选择字段面向连接的数据完整性。
- 选择字段无连接的数据完整性。
- 无连接的数据完整性。

（4）数据保密性服务

采用数据保密性服务的目的是保护网络中各通信实体之间交换的数据，即使被非法攻击者截获，也无法解读信息内容，以保证信息不失密。该服务也提供面向连接和无连接两种数据保密方式。保密性服务还提供给用户可选字段的数据保护和信息流安全，即对通过观察信息流就可能推导出的信息提供保护。信息流安全的目的是确保信息从源点到目的点的整个流通过程的安全。

（5）非否认服务

非否认服务可防止发送方发送数据后否认自己发送过数据，也可防止接收方接收数据后否认自己接收过数据。它由源点非否认服务和交付非否认服务两种服务组成。这实际上是一种数字签名服务。

表 1.1　　与网络各层相关的 OSI 安全服务

安全服务		OSI 层次						
		1	2	3	4	5	6	7
鉴别服务	同等实体鉴别			√	√			√
	数据源鉴别			√	√			√
访问控制	访问控制服务			√	√			√
数据完整性	带恢复功能的连接完整性	√			√			√
	不带恢复功能的连接完整性			√	√			√
	选择字段连接完整性							√
	选择字段无连接完整性			√	√			√
	无连接完整性							√
数据保密性	连接保密性	√	√	√	√		√	√
	无连接保密性		√	√	√		√	√
	信息流保密性	√		√				√
非否认服务	发送非否认							√
	接受非否认							√

注：“√”表示提供安全服务，空白表示不提供安全服务