普通高等教育“十二五”规划教材（高职高专教育）

网络安全技术实用教程

（第二版）

谭方勇　田　涛　主　编
周　莉　张　燕　副主编

中国电力出版社
CHINA ELECTRIC POWER PRESS

普通高等教育“十二五”规划教材（高职高专教育）

网络安全技术实用教程

（第二版）

主　编　谭方勇　田　涛
副主编　周　莉　张　燕
编　写　肖长水
主　审　孟东升

中国电力出版社
CHINA ELECTRIC POWER PRESS

内 容 提 要

本书为普通高等教育“十二五”规划教材（高职高专教育）。全书共11个项目，主要包括网络安全项目介绍与分析、网络协议基础、网络攻击与防范、操作系统安全配置、网络病毒的清除与预防、密码技术分析与应用、数字签名技术分析与应用、VPN技术应用、Web安全和电子商务、防火墙安全配置和典型网络安全方案设计等内容。

本书可作为全国高职高专院校、成人高校及本科院校举办的二级职业技术学院计算机相关专业的教材，也可作为网络安全技术的培训教材或自学参考书，对于网络管理员和网络工程技术人员也有一定的参考价值。

图书在版编目（CIP）数据

网络安全技术实用教程 / 谭方勇，田涛主编. —2版. —北京：中国电力出版社，2011.8

普通高等教育“十二五”规划教材. 高职高专教育

ISBN 978-7-5123-2020-8

Ⅰ. ①网… Ⅱ. ①谭… ②田… 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（2011）第163388号

中国电力出版社出版、发行

（北京市东城区北京站西街19号 100005 http://www.cepp.sgcc.com.cn）

北京丰源印刷厂印刷

各地新华书店经售

*

2008年7月第一版

2011年9月第二版 2011年9月北京第四次印刷

787毫米×1092毫米 16开本 18.5印张 449千字

定价 **32.00** 元

前　言

随着计算机技术及信息技术的迅猛发展，计算机网络在人们的工作、学习和生活中占据了非常重要的地位，同时也推动了社会的发展。但是，目前计算机网络特别是 Internet 上网络及其信息的安全问题日益突出，计算机网络安全及信息安全的问题也成为人们关注的重点之一，这不仅给用户对网络使用带来了不便，而且还给个人、企业和社会造成了巨大的损失。可见计算机网络的安全也变得越来越重要。

本书采用任务驱动的项目式教学为编写思路，注重网络安全的理论知识和实际的项目案例相结合，具有很强的可操作性，注重理论与实践的结合，每个项目分为学习目标、背景知识、工作任务、任务实施、问题分析等几个模块，既给出了完成这个项目的学习目标和主要工作任务，又给出了完成该项目需要的理论知识，然后按照给定的工作任务来实施项目，完成后对实施过程中出现的问题进行分析。

本书在第一版的基础上，对近年来网络安全技术与应用的新成果进行概括和完善，采用新的基于任务驱动的项目式教学手段为设计思路，并采用通俗易懂的语言，围绕网络安全技术的主要问题进行阐述。

作者根据多年从事计算机网络安全教学、科研和网络管理工作的实践经验编写了此书，在编写的过程中，力求使本书具有以下特色：

（1）内容体系架构为知识基础维、技术基础维和综合能力维螺旋式上升的三维课程整合模式。

（2）注重理论与实践相结合，以项目案例形式让读者掌握每一个知识点的应用，并提高实际的操作技能。

（3）突出教材内容的系统性、先进性，项目案例的可操作性、实用性。

本书由苏州市职业大学的谭方勇、北京首都国际机场股份有限公司的田涛主编，设计了本教材的改编思路，对大纲进行了总体策划，指导全书的编写工作；苏州市职业大学的周莉、张燕副主编；苏州市职业大学的肖长水参编。谭方勇编写项目 1、项目 4、项目 10；田涛编写任务 11.1 和任务 11.2；张燕编写项目 3、项目 5 和任务 11.3；周莉编写项目 2、项目 8 和项目 9；肖长水编写项目 6 和项目 7。全书由西安石油大学孟东升主审。

限于编者水平，加之时间仓促，书中错漏和不足之处在所难免，恳请广大读者批评指正。编者 E-mail 地址为 tanfy@126.com。

编　者

2011 年 6 月

目　录

项目 1　网络安全项目介绍与分析

随着 Internet 技术的日益发展和普及，计算机网络作为一种重要的信息传送手段，对我们的工作和生活起着越来越重要的作用。但是，网络安全问题也同样到了令人担忧的地步。目前，利用计算机网络进行各种违法行为的事件在不断出现，网络黑客攻击，计算机病毒、木马、蠕虫等字眼在我们眼前出现的概率也越来越高。因此，计算机网络安全问题必须得到重视。

本项目主要根据当前网络安全的状况做出安全需求分析，并结合网络安全的评价标准及网络安全防御体系的一般结构来制定相关网络（如校园网、企业网、政府网等）的安全方案规划。最后，对后续的网络安全实验进行设计并建立一个虚拟的实验环境。

任务 1.1　网络安全需求分析

任务 1.1.1　了解网络安全的发展历史

1. 学习目标

（1）了解网络安全问题的产生背景。

（2）分析网络安全的现状。

（3）了解网络安全的发展趋势。

2. 背景知识

（1）网络安全问题的产生。计算机网络尤其是 Internet 具有较强的开放性、分散性和交互性的特点，这样的网络环境为信息共享、信息服务和信息交流提供了非常便捷的空间。因此网络技术得到了迅速的发展和广泛的应用，也为人类社会的进步起到了巨大的推动作用。但也正是由于它的这些特点，随之带来了很多安全问题，主要表现如下：

1）信息泄露、信息污染、信息不可控等，如资源未授权访问、未授权信息流出现、系统拒绝信息流和系统否认等。

2）某些个人或者组织出于某种特殊目的进行信息泄露、信息破坏、信息假冒侵权和意识形态的信息渗透，甚至进行一些破坏国家、社会及各类主体合法权益的活动。

3）随着社会的高度信息化，社会的“命脉”和核心控制系统有可能面临恶意的攻击而导致损坏和瘫痪，如金融系统、政府网站、国防通信设施等。

4）网络应用越来越广泛，但是控制权分散的管理问题也日益显现。由于人们利益、目标和价值的分歧，使信息资源的保护和管理出现脱节，这也使得信息安全问题变得广泛而复杂。

（2）网络安全的现状。目前各种领域的计算机犯罪和网络侵权行为在数量、规模、手段等方面都已经到了令人吃惊的地步。据统计，目前美国每年由于网络安全问题而遭受的经济损失超过 170 亿美元；德国、英国也均在数十亿美元以上；法国、日本、新加坡问题也很严重。在国际刑法界列举的现代社会新型犯罪排行榜上，计算机犯罪已名列榜首。另外，全球平均每 20s 就会发生 1 次网络入侵事件。我国的网络安全事件的发生率也在不断上升。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 年上半年，CNCERT 共处理各类网络安全事件 784 件，比去年同期增长了 92.16%。CNCERT 处理的事件类型主要有恶意代码、网页仿冒、网页篡改等。各类事件处理数量分布如图 1-1 所示[1]。在 CNCERT 处理的网络安全事件中，涉及金融企业、重要商业机构的网页仿冒类事件最多，网页挂木马及网页篡改事件也较频发，特别是针对国内政府机构和重要信息系统部门的网页挂木马和网页篡改事件。

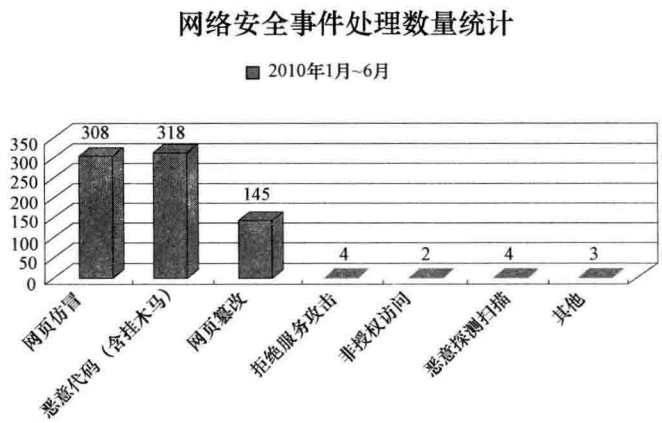

图 1-1　2010 年上半年 CNCERT 处理的网络安全事件数量统计

（3）网络安全的发展趋势。黑客攻击技术与病毒技术相融合，使得未来网络安全的形势也非常严峻，主要表现在以下几个方面：

1）实施网络攻击的主体的变化。目前网络攻击行为已经从原先的由好奇心重、喜欢炫耀攻防能力的兴趣型黑客群向更具犯罪思想的盈利型的攻击人群过渡，利用操作系统漏洞实施“Zero-day 攻击”和利用网络攻击获取经济利益已逐步成为主要趋势。另外，以僵尸网络、间谍软件为手段的恶意代码攻击，以敲诈勒索为目的的分布式拒绝服务攻击（DDoS），以网络仿冒、网址嫁接、网络劫持等方式进行在线身份窃取等安全事件也不断增加。而针对 P2P、IM 等新型网络应用的安全攻击也在快速发展。曾经的“熊猫烧香”、“灰鸽子”等病毒事件形成的黑色产业链也凸显了解决网络安全问题的重要性和紧迫性。

2）网络攻击的主要手段的变化。网络攻击的手段很多，主要包含拒绝服务攻击、非法接入、IP 欺骗、网络嗅探、中间人攻击、木马攻击及信息垃圾等。随着攻击技术的不断发展，攻击的手段也由原来单一的攻击手段向结合多种攻击手段的综合性攻击发展。如网络嗅探、拒绝服务、木马等攻击手段的结合将带来更大的危害。

3）企业内部对安全威胁的认识的变化。企业网络安全的防护中心以前一直定位于网络边界及核心数据区，通过部署各种安全设备实现安全保障。但是，随着企业网络边界安全体系的基本完善，网络安全事件仍然不断发生。内部员工安全管理上的不足和员工上网使用不当等行为带来的安全风险更为严重。因此企业管理人员也逐步认识到加强内部安全管理、采取相关的安全管理技术手段控制企业网络安全风险的重要性。

[1] CNCERT/CC 2010 年上半年网络安全工作报告。

3. 工作任务

（1）通过 Internet 搜索历史上相关网络安全事件，并分析导致其发生的主要原因。

（2）通过 Internet 搜索权威机构发布的安全事件统计情况，并对安全事件发展的趋势做出分析。

任务 1.1.2　了解计算机网络安全的定义及评价标准

1. 学习目标

（1）理解对计算机网络安全的定义。

（2）熟悉计算机网络安全的评价标准。

2. 背景知识

（1）计算机网络安全的定义。计算机网络安全是集合了计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多门学科的一门综合性学科。

计算机网络安全的主要目标是保护计算机网络系统中的软件、硬件及信息等资源，使其不会因为偶然的或者恶意的原因而遭到破坏、更改、泄露，系统可以连续可靠地正确运行，网络服务不被中断。

计算机网络安全应具备的几个特征如下：

1）保密性：防止在网络上传递的信息泄露给非授权用户、实体或过程，信息只提供给授权用户使用。

2）完整性：保证网络上传输的信息在存储、传输过程中不被篡改。

3）可靠性：保证计算机网络系统能够在规定的条件下及规定的时间内完成规定的功能。

4）可用性：保证被授权实体能够访问所需要的信息。

5）可控性：对网络信息的传播及内容具有控制能力。

6）不可抵赖性：对出现的安全问题能够提供依据与手段。

（2）计算机网络安全的评价标准。在国际上，发布于 1985 年的美国国防部可信计算机系统评价标准（Trusted Computer Standards Evaluation Criteria，TCSEC），即网络安全橙皮书，是世界上第一个关于信息产品安全的评价标准。其他各个国家也根据自己的国情制定了相关的标准。

1）国际评价标准：自从网络安全橙皮书成为美国国防部的标准以来，它一直是作为评估多用户主机、小型操作系统、数据库系统、计算机网络系统的主要方法。橙皮书把安全的级别从低到高分成 4 个类别：D 级、C 级、B 级和 A 级，其中每级又分几个子级，如表 1-1 所示。

表 1-1　　橙皮书的安全级别

类别	级　别	名　　称	主　要　特　征
D	D	低级保护	没有安全保护
C	C1	自主安全保护	自主存储控制
	C2	受控存储控制	单独的可查性，安全标识
B	B1	标识的安全保护	强制存取控制，安全标识
	B2	结构化保护	面向安全的体系结构，较好的抗渗透能力
	B3	安全区域	存取监控、高抗渗透能力
A	A	验证设计	形式化的最高级描述和验证

其中，D 级安全等级最低，它只给文件和用户提供安全保护，对于硬件来说，是没有任何保护措施的。操作系统容易受到损害，没有系统访问限制和数据访问限制，任何人不需任何账户都可以进入系统，不受任何限制可以访问他人的数据文件。属于这个级别的操作系统有 DOS 和 Windows 98 等。

C 级中有 C1 和 C2 两个子级。其中，C1 系统的可信计算基础体制通过将用户和数据分开来达到安全的目的。这种级别的系统对硬件又有某种程度的保护，如用户拥有注册账号和口令，系统通过账号和口令来识别用户是否合法，并决定用户对程序和信息拥有什么样的访问权，但硬件受到损害的可能性仍然存在。

用户拥有的访问权是指对文件和目标的访问权。文件的拥有者和超级用户可以改变文件的访问属性，从而对不同的用户授予不同的访问权限。

C2 级除了包含 C1 级的特征外，C2 级应该具有访问控制环境（Controlled-access Environment）权力。该环境具有进一步限制用户执行某些命令或者访问某些文件的权限，而且还加入了身份认证等级。另外，系统对发生的事情加以审核，并写入日志中，如什么时候开机，哪个用户在什么时候从什么地方登录等。这样通过查看日志，就可以发现入侵的痕迹。如发现多次登录失败信息，表明可能有人尝试入侵系统。审计除了可以记录系统管理员执行的活动以外，还加入了身份认证级别，这样就可以知道谁在执行这些命令。但审计的缺点在于它需要额外的处理时间和磁盘空间。

能够达到 C2 级的常见操作系统有 UNIX 系统、Novell 3.x 或者更高版本、Windows NT、Windows 2000 和 Windows 2003。

B 级中有三个级别。B1 级，又称标志安全保护级别（Labeled Security Protection），是支持多级安全（如秘密和绝密）的第一个级别。这个级别说明处于强制性访问控制之下的对象，系统不允许文件的拥有者改变其许可权限。

安全级别存在保密级别、绝密级别，这种安全级别的计算机系统一般在政府机构中。

B2 级，又称结构保护级别（Structured Protection），它要求计算机系统中所有的对象都要加上标签，而且给设备（磁盘、磁带和终端）分配单个或者多个安全级别。

B3 级，又称安全域级别（Security Domain），使用安装硬件的方式来加强域的安全。例如，内存管理硬件用于保护安全域免遭无授权访问或更改其他安全域的对象。该级别也要求用户通过一条可信任途径连接到系统上。

A 级，又称验证设计级别（Verified Design），是当前橙皮书的最高级别，它包含了一个严格的设计、控制和验证过程。该级别包含了较低级别的所有安全特性。

在美国发表 TCSEC 之后，欧洲各国也进行了信息技术的安全问题研究，同时也发布了自己的信息技术安全评价标准。例如，在英国，CESG 备忘录 3 提供给政府部门使用，工商部的建议“绿皮书”提供给信息技术安全产品作为参考。德国的信息技术安全局在 1989 年发布了自己的标准。同年，法国也发布了自己的标准“蓝—白—红书”。

为了统一标准，1991 年德国、法国、荷兰和英国等国家共同发布了“信息技术安全评价标准（Information Technology Security Evaluation Criteria, ITSEC）V1.2”。

2）国内评价标准：1999 年 10 月，我国根据《计算机信息系统安全保护等级划分准则》并经过国家质量技术监督局批准发布，将计算机安全保护划分为以下五个级别。

第一级：用户自主保护级，它的安全保护机制使用户具备自主安全保护的能力，保护用

户的信息免受非法的读/写破坏。

第二级：系统审计保护级，除具备第一级所有的安全保护功能外，要求创建和维护访问的审计跟踪记录，使所有的用户对自己行为的合法性负责。

第三级：安全标记保护级，除继承前一个级别的安全功能外，还要求以访问对象标记的安全级别限制访问者的访问权限，实现对访问对象的强制保护。

第四级：结构化保护级，在继承前面安全级别安全功能的基础上，将安全保护机制划分为关键部分和非关键部分，对关键部分直接控制访问者对访问对象的存取，从而加强系统的抗渗透能力。

第五级：访问验证保护级，增设了访问验证功能，负责仲裁访问者对访问对象的所有访问活动。

3. 工作任务

（1）举例说明计算机网络安全是一门集多门学科于一体的综合性学科。

（2）说明计算机网络安全的评价标准对网络安全建设的主要意义。

任务 1.1.3　认识网络安全的威胁

1. 学习目标

（1）了解网络安全的威胁因素。

（2）理解网络安全的分类。

2. 背景知识

Internet 作为信息时代的重要标志已经深入渗透到现实世界的政治、经济、文化、军事和科技等许多领域，每个国家都开始将网络作为领土、领海、领空后的新的安全空间。很多国家都已经加强在网络安全维护力量上的建设，努力通过各种措施来防范和遏制网络对国家安全造成威胁。据美国 FBI 统计，83%的网络安全事故是由内部人员与外部人员勾结而造成的。而据我国公安部统计，70%的泄密犯罪来自内部。

（1）威胁网络安全的主要因素。

1）管理因素：管理是维护一个网络安全的重要因素。责权不明、管理者素质低下、用户安全意识淡薄、管理制度不健全或可操作性差等都会使网络受到安全威胁。例如，网络在受到攻击或其他一些安全威胁时无法进行实时的检测、监控、报告和预警。

2）技术因素：网络中主要的对象（如操作系统、软件及通信协议等）本身存在的安全漏洞；加密和解密、入侵检测技术等相关安全产品仍不完善；病毒的千变万化、层出不穷；黑客程序在网络上的肆意传播等技术问题都是当前网络安全中不可避免的威胁因素。

3）人为因素：人为的无意失误，如用户的安全设置不当造成的安全漏洞，用户的空口令或弱口令，没有访问关键系统权限的员工因误操作而进入关键系统都会对网络安全造成威胁。人为的攻击，如以各种方式有选择地破坏信息的完整性和有效性的主动攻击或在不影响正常工作下进行窃取、截获重要机密信息的被动攻击等。

（2）网络安全威胁的种类。网络安全威胁主要可以分成以下三类。

1）非授权访问：即没有事先经过同意，通过假冒身份攻击、系统漏洞等手段来获取系统的访问权限，从而使非法用户进入网络系统来使用网络资源，造成资源的消耗或损坏，损害合法用户的利益。

2）拒绝服务攻击：拒绝服务（Denial of Service，DoS）是一种破坏性的攻击，而且危害性很大，攻击者通过某种方法使得系统响应减慢甚至瘫痪，从而阻止合法用户获得服务。

拒绝服务攻击不需要高级的技术和技巧，也不需要目标服务器的任何访问权限，因此发动攻击相对比较简单，而且发生的概率也有不断增加的趋势。到目前为止还没有一种很好的方法来确认攻击者的身份。

3）数据欺骗：主要包括捕获、修改和破坏可信主机上的数据。攻击者还有可能对通信线路上的网络通信进行重定向。另外，协议和操作系统内在的缺陷也有可能导致上述问题。这种攻击的一个典型例子就是对 Web 站点的攻击，在此类攻击中，攻击者往往会修改网页的内容，从而达到欺骗网络用户的目的。

3. 工作任务

（1）对当前网络的主要应用服务存在的安全威胁进行分析，如针对企业 Web 2.0 应用的安全威胁（病毒、僵尸网络、路过式下载、恶意软件、钓鱼攻击、特洛伊木马等）。

（2）根据当前网络及其相关应用的发展趋势，分析未来网络安全的主要威胁因素，如移动办公网络、虚拟化技术、云计算等。

（3）试说明作为一个网络管理者或是一个普通用户，如何来应对存在的网络安全威胁。

任务 1.1.4 理解网络安全的脆弱性

1. 学习目标

理解网络安全脆弱性的原因。

2. 背景知识

脆弱性主要是指计算机网络系统在硬件、软件、协议设计与实现，以及系统采取的安全策略等存在的不足或缺陷。它的存在会导致非授权用户能够获取或提高访问权限，从而破坏网络系统。

（1）操作系统安全的脆弱性：操作系统的体系结构本身就存在安全问题，这也是计算机系统不安全的根本原因。例如，目前主流的操作系统（如 Windows 系统、UNIX 系统）的 I/O 驱动程序及系统服务都可以利用升级补丁的方式进行动态链接，这使得病毒可以很方便地利用它来入侵操作系统，从而使系统变得脆弱。系统提供的 Debug 和 Wizard 等程序可以将执行程序进行反汇编，从而对程序的执行过程进行跟踪，这也经常被黑客所利用。

（2）网络协议的脆弱性：TCP/IP 是目前 Internet 的核心协议，它还包含了 FTP、Telnet、RPC、NFS、SMTP 等协议。由于 TCP/IP 形成于网络诞生之初，所以在设计上遵循的是简单实用的原则，因此在网络安全方面的考虑存在着不足，特别是面对当今规模日益庞大的 Internet，其在网络安全上的脆弱性逐渐显现。

（3）数据库系统的脆弱性：目前网络上大部分商业应用都要依赖数据库系统，然而数据库的安全管理跟操作系统一样，建立在分级管理的概念之上，所以它的安全性也相对比较脆弱。

（4）应用软件的脆弱性：应用软件在设计和实现时，程序员可能由于编程的疏忽或为了自我方便而设计了一些后门，从而留下了很大的安全隐患。

（5）安全管理的脆弱性：对现有信息系统大多都缺少安全管理员，缺少安全管理的技术规范，缺少定期的安全检测，更缺少安全监控，这使得安全管理也变得脆弱。

3. 工作任务

（1）列举因 Windows、Linux 等操作系统本身的脆弱性而导致的历史安全事件。

（2）列举因网络协议的脆弱性而导致的历史安全事件。

（3）列举因数据库系统的脆弱性而导致的历史安全事件。

任务 1.2　网络安全方案规划

任务 1.2.1　了解网络安全防御体系结构

1. 学习目标

（1）了解一套科学、可行的网络安全防御体系的重要性。

（2）熟悉网络安全防御体系的层次结构。

2. 背景知识

安全防御体系应该是融合了技术体系和管理体系的解决网络安全问题的体系，它具备全面性、过程性、动态性、层次性和平衡性等特性。一个完整的安全防御体系应该根据网络应用的整体现状，建立以安全策略为核心，以安全技术为保障，以安全管理为手段的全方位、动态的安全防御系统。所以，在整个体系中，安全策略、安全技术及管理手段是非常重要的环节。

（1）安全策略。安全策略是整个安全防御体系的核心，它是对来自网络内外的安全威胁进行防御的安全措施的集合，一般它遵循动态性、简单性和系统性等原则，从网络分层结构的角度来对网络各个层次的安全状况提出相应的安全策略。

1）物理层和链路层：在这两层之上主要是保证信息传输的安全性、完整性和可获性，改善通信链路的性能，使其能够最大限度地提供可靠、通畅及便捷的数据链路。而安全策略主要考虑的因素有通信介质、主机等物理设备、机房安全和人为破坏等。

2）网络层：主要涉及交换与路由相关设备。安全策略主要考虑网络信息的安全性，包括网络身份认证、网络资源的访问控制、数据传输的保密与完整性、远程接入的安全、域名系统的安全、路由系统的安全、防火墙应用、病毒防范和入侵检测等手段。

3）操作系统层：在此层，安全策略主要考虑的因素包括操作系统的安全配置、操作系统的漏洞检测、操作系统的漏洞修补等，它是衡量网络操作系统安全性、可靠性的依据。

4）应用层：应用层的安全策略主要考虑业务网络对用户提供服务所采用的应用软件和数据的安全性。应用层安全要求能保护合法用户对数据的合法存取，阻止非法用户对数据进行非授权的访问、转移、修改和破坏。它包括身份认证、访问控制、数据库系统中数据的安全性等几方面。

（2）安全技术。常见的安全技术主要包括访问控制技术、数据加密技术、防火墙技术、入侵检测技术、审计跟踪技术、病毒防范技术、扫描评估技术、备份还原技术等。

1）访问控制技术：是网络安全防御的主要策略之一，主要保证网络资源不被非授权使用和访问。访问控制技术主要包含入网访问控制、网络权限控制、目录级控制及属性控制等手段。

2）数据加密技术：是实现网络安全的主要策略之一，是实现分布式系统和网络环境下数

据安全的重要手段。它的核心内容就是密码学，其中包括数据加密、数字签名、身份认证、密钥管理等内容。

3）防火墙技术：建立在现代通信技术和信息安全技术基础上的应用性安全技术，它一般被设置在不同网络（如可信的企业内部网络和不可信的公共网络）或网络安全域之间，是一系列部件的组合，主要包括包过滤、服务访问策略、验证工具和应用网关等几部分。

4）入侵检测技术：能够识别针对计算机或网络资源的恶意企图或行为，并对此做出相应反应的安全技术。它能够检测非授权对象针对系统的入侵企图或行为，同时监控授权对象对系统的非法操作。

5）审计跟踪技术：一种在安全事件发生后进行追查的主要手段，它能对涉及计算机操作系统、数据库管理系统、网络管理系统等系统的操作进行完整记录，以便实时地监控、报警或进行事后分析、统计、报告，通过事后查询来保证系统安全。

6）病毒防范技术：主要可以通过杀毒工具、系统及软件漏洞的修补，以及规范的操作行为来防范病毒对客户端及服务器的感染。

7）扫描评估技术：一项主动检测网络系统漏洞的技术，它模拟黑客的攻击方法对目标系统（如服务器、数据库系统、网络设备、工作站等）可能存在的安全漏洞进行检测，并给出安全分析报告，指出系统存在的漏洞和相关弥补措施和建议，为提高网络安全的整体水平提供重要依据。

8）备份还原技术：灾难备份与还原技术，它利用技术、管理手段及相关资源来确保关键数据能够在灾难发生后尽可能地还原。

（3）管理手段。完善的网络管理手段是网络安全技术和安全策略的有效补充，使得整个网络安全防御体系更可靠、更安全。而网络安全管理制度是其中一个重要的措施，应该组织相关工作人员认真学习《计算机信息网络国际互联网安全保护管理办法》，提高其维护网络安全的自觉性和警惕性。

（4）安全防御体系的设计模型。网络安全防御体系是一个动态的、基于时间变化的概念。为确保网络与信息系统的抗攻击性能，保证信息的完整性、可用性、可控性和不可否认性，在设计网络安全防御体系时需结合不同的安全保护因素，如防火墙、防毒软件和安全漏洞检测工具，来创建一个比单一防护更有效的综合保护屏障。多层、安全互动的安全防护将大大增加黑客攻击的难度和成本，因此他们对网络系统的攻击也将大大减弱。如图 1-2 所示，为一个网络安全防御的基本模型。

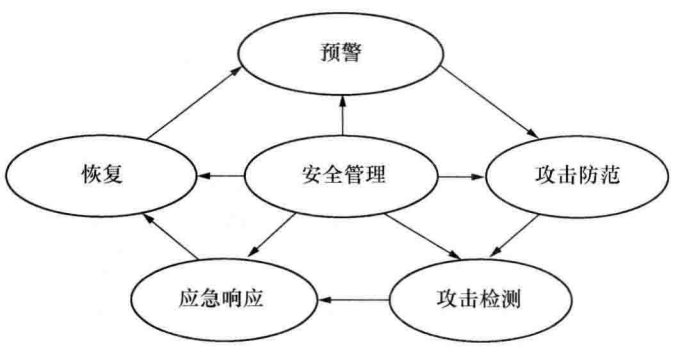

图 1-2　网络安全防御的基本模型

（5）网络安全防御体系工作流程。本过程主要分为三个步骤，即攻击前的防范、攻击工程中的防范及攻击过后的恢复处理。

1）攻击前的防范，主要是负责对日常的防御工作及对实时的消息进行防御。一般防火墙作为第一道防范，负责控制进入网络的访问控制，既进行了日常的防御工作，也对实时的消息进行防御。接着，系统漏洞检测系统和安全评估软件，一个从内一个从外，详细地扫描安全漏洞并一一列举系统的漏洞，并给出最佳解决方法。另外，邮件过滤系统、PKI、VPN 等都是进行日常的防御工作。

2）攻击过程中的防范，主要负责对实时的攻击做出反应。预警系统和入侵检测系统检测通过防火墙的数据流，并进行进一步检查，综合分析各种信息，动态分析出哪些是黑客对系统做出的进攻，并立即做出响应。通过分析系统审计日志中大量的跟踪用户活动的细节记录来发现入侵，分别在网络级和系统级上共同探测黑客的攻击并及时做出反击，防止黑客进行更深一步的破坏。

3）攻击过后的恢复处理，攻击过后的应对部分主要是在造成一定损害时，由应急响应与灾难恢复子系统进行处理。

3. 工作任务

（1）以某一种类型的网络为背景（如办公网络、网吧、宿舍网络等），为其设计安全防御系统方案。

（2）说明网络管理手段在公司网络管理中的必要性。

任务 1.2.2　网络安全的规划

1. 学习目标

（1）明确进行网络安全规划的目的。

（2）确定网络安全规划的内容及一般步骤。

2. 背景知识

（1）规划的依据。网络安全的规划一定要依据相关的法规和标准来进行，这也是保证网络安全的一个前提条件。主要的法规如下：

1）GB/T 22080—2008 《信息技术安全技术信息安全管理体系要求》（ISO/IEC 27001：2005）。

2）GB/T 22081—2008 《信息技术安全技术信息安全管理实用规则》（ISO/IEC 27002：2005）。

3）ISO/IEC TR 15443：2005《信息技术安全保障框架》。

4）ISO/TEC 13335：2004《信息技术安全管理指南》。

（2）规划的主要内容。网络安全规划的主要内容一般分为以下几个方面：

1）物理安全规划，主要包含环境安全、设备安全、介质安全等方面。

2）网络安全规划，主要包括网络安全区域的划分、制定安全的访问控制策略等。

3）主机与系统安全规划，主要包括系统的加固、病毒防护、防止信息泄露、补丁升级等。

4）应用安全规划，主要包括各类应用服务器的安全规划。

5）数据安全规划，主要包括各类数据库服务器的安全规划。

（3）规划的一般步骤。网络安全规划的一般步骤需要根据当前网络系统的现状来分析其

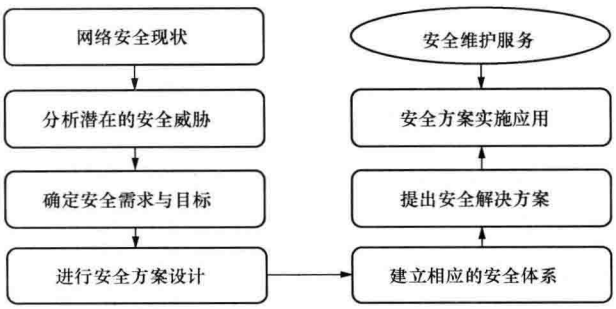

图 1-3 网络安全规划的一般流程

中潜在的威胁因素，然后提出相应的安全需求与目标，之后才能进行安全方案的设计及安全体系的建立，然后提出安全解决方案，最后再对该方案进行实施应用，具体流程如图 1-3 所示。

3. 工作任务

（1）对当前网络系统进行安全需求分析与风险分析，提出安全需求与目标。

（2）对当前网络系统的网络进行规划，确定子网划分与虚拟子网划分的方案。

（3）提出对当前网络系统的安全访问控制策略的建议。

（4）提出对当前网络系统的备份与恢复方案。

（5）建立一套应急事件处理规程。

任务 1.3 网络安全项目环境设计

任务 1.3.1 网络拓扑图设计

1. 学习目标

（1）掌握网络拓扑图的设计方法。

（2）掌握 Microsoft Visio 的网络拓扑图的绘制方法。

2. 背景知识

在网络工程的建设中，网络拓扑图是网络工程师实施网络建设方案的一张图纸。同时，在日常的网络管理中，网络拓扑图又成为网络管理员管理网络的一个必备工具，它能帮助管理员更清楚地了解所管网络的所有网络设备的真实连接情况、子网划分情况、设备分布情况、运行情况、连接状态及链路负载等情况，从而快速地解决网络问题。

（1）网络拓扑图设计工具。对于网络拓扑图的绘制工具有很多，结构简单的拓扑图可以通过 Microsoft Word 中的绘图工具或 Windows 系统的“画图”程序完成。对于结构复杂、规模较大的网络拓扑结构图，则可以通过微软公司的 Microsoft Visio 等软件完成。

Microsoft Visio 是微软公司开发的一款高级绘图软件，它可以绘制流程图、网络拓扑图、组织结构图等，也可以帮助网络工程师创建商业和技术方面的图形，对复杂的概念、过程及系统进行组织和文档备案。

（2）网络拓扑图的设计原则。网络拓扑图的设计主要是确定各种设备以何种方式连接起来。根据企业的网络规模、网络体系结构、采用的协议及扩展和升级管理等多个方面来进行考虑。网络拓扑结构设计的好坏直接影响到网络的整体性能。

局域网常用的拓扑结构主要有总线型、星型、环型及混合型拓扑等，不同的网络控制策略（即网络数据的传输方式、通信协议和控制方法）所使用的网络连接设备也不相同，所以，在网络规划或设计时必须首先确定网络的拓扑结构。

3. 工作任务

（1）为 Microsoft Visio 2003 添加思科 Cisco、锐捷 Ruijie 等设备厂商的产品图标。

（2）使用 Microsoft Visio 2003 绘制网络安全方案拓扑图，如图 1-4 所示。

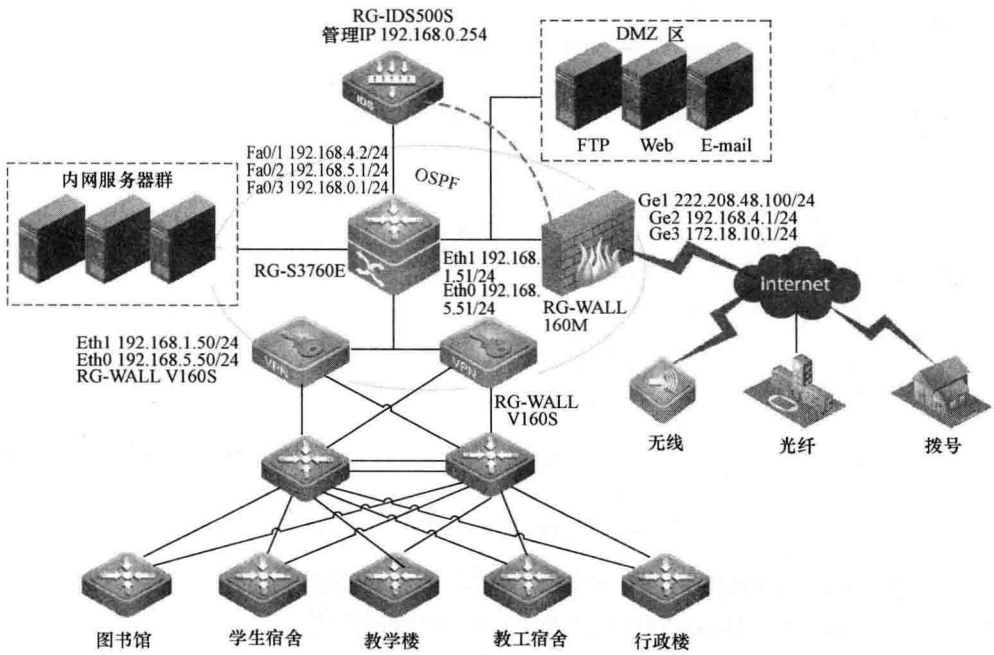

图 1-4　网络安全方案拓扑图

4. 任务实施

利用 Microsoft Visio 2003 来设计如图 1-4 所示的网络拓扑的过程如下。

（1）下载产品图标。Microsoft Visio 2003 具有丰富的设备图标，但是为了更形象地表示方案中的产品，在本次任务中将用设备厂商提供的图标。可以通过 Internet 的搜索引擎查找并下载支持 Microsoft Visio 2003 的图标文件（*.vss）。如图 1-5 所示为锐捷网络设备产品的图标。

名称	修改日期	类型	大小
RG安全产品.vss	2009/8/25 19:10	Microsoft Visio 模具	496 KB
RG办公设备.vss	2009/8/25 19:31	Microsoft Visio 模具	299 KB
RG存储产品.vss	2009/8/25 19:22	Microsoft Visio 模具	2,283 KB
RG服务器.vss	2009/8/25 19:25	Microsoft Visio 模具	440 KB
RG交换机.vss	2009/8/25 19:03	Microsoft Visio 模具	160 KB
RG路由.vss	2009/8/25 18:58	Microsoft Visio 模具	172 KB
RG其它.vss	2009/8/25 19:31	Microsoft Visio 模具	339 KB
RG数据库.vss	2009/8/25 19:26	Microsoft Visio 模具	1,441 KB
RG无线产品.vss	2009/8/25 19:06	Microsoft Visio 模具	389 KB

图 1-5　锐捷网络设备产品的图标

（2）运行 Microsoft Visio 2003。在“开始”→“程序”菜单中，单击展开 Microsoft Office 菜单，单击运行 Microsoft Office Visio 2003 程序，进入 Microsoft Visio 2003 程序主界面，如