21世纪高职高专计算机类专业规划教材

网络安全技术实用教程

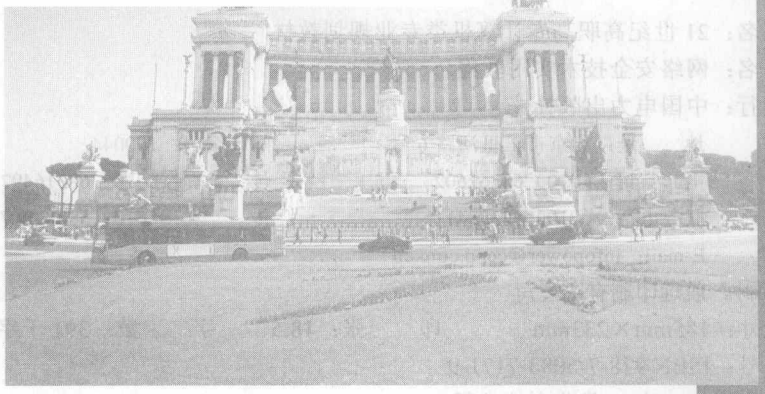
■ 谭方勇 主 编
■ 周 莉 张 燕 副主编

中国电力出版社
www.infopower.com.cn
中国电力出版社 CHINA ELECTRIC POWER PRESS

21世纪高职高专计算机类专业规划教材

网络安全技术实用教程

■ 谭方勇 主 编
■ 周 莉 张 燕 副主编
■ 肖长水 陆 侃 于复生 参 编



中国电力出版社
www.infopower.com.cn

内容提要

本书采用理论与实践相结合的案例教学方式，结合完整清晰的操作步骤，全面介绍了计算机网络安全基础、网络协议基础、网络攻防技术应用、操作系统安全配置方案、计算机病毒及防治技术、密码技术应用、数字签名技术应用、VPN 技术应用、Web 安全和电子商务、防火墙技术应用、计算机网络攻击应急响应和网络安全方案设计等知识。

本书可以作为高职高专院校的相关专业的网络安全课程教材和参考书，适合各单位网络管理员、网络工程技术人员以及广大网络爱好者阅读和参考。

图书在版编目（CIP）数据

网络安全技术实用教程/谭方勇主编. —北京：中国电力出版社，2008
21 世纪高职高专计算机类专业规划教材
ISBN 978-7-5083-7171-9

Ⅰ. 网… Ⅱ. 谭… Ⅲ. 计算机网络—安全技术—高等学校：技术学校—教材 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2008）第 094649 号

丛 书 名：21 世纪高职高专计算机类专业规划教材
书　　名：网络安全技术实用教程
出版发行：中国电力出版社
地　　址：北京市三里河路 6 号　　邮政编码：100044
电　　话：（010）68362602　　传　　真：（010）68316497，88383619
服务电话：（010）58383411　　传　　真：（010）58383267
E-mail：infopower@cepp.com.cn
印　　刷：航远印刷有限公司
开本尺寸：185mm×233mm　　印　　张：18.5　　字　　数：391 千字
书　　号：ISBN 978-7-5083-7171-9
版　　次：2008 年 7 月北京第 1 版
印　　次：2008 年 7 月第 1 次印刷
印　　数：0001—3000 册
定　　价：28.00 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互联网（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，这不仅给用户使用网络带来了不便，而且还给个人、企业和社会造成了巨大的损失。所以计算机网络的安全也变得越来越重要。

本书注重网络安全的理论知识和实际的网络安全案例相结合，具有很强的可操作性，注重理论与实践的结合，每章都配以相应的案例来进行知识点讲解，同时还提供了实验或实践项目的说明。

本书内容主要分为三部分：①计算机网络安全基础，主要介绍网络安全的基本理论、网络安全实验环境的搭建、网络协议分析基础等；②计算机网络安全攻击与防御技术，主要介绍网络安全的攻击与防御技术、操作系统安全、计算机病毒及防治、密码技术及认证系统、VPN、Web 服务器安全及防火墙技术应用等；③网络安全综合案例解决方案，主要介绍网络安全的需求分析以及针对实际网络工程安全方案的设计。

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 5 个特点。

（1）灵活性：本书的目的是向学生提供尽可能灵活、创新的教学方法和学习途径。培养读者的网络安全技术实践能力。

（2）新颖性：本书在内容上体现技术上的新颖，将介绍一些最新的网络安全技术。

（3）实用性：本书的内容尽可能体现网络安全的实际，将介绍必备的网络安全知识和实用技巧，锻炼读者的网络安全能力。

（4）多实例：以现实安全实例为背景，列举大量的案例和实践项目，提供最新的网络安全技术。

（5）利教学：提供每章的大纲及章节内容的教学提示和培养目标，提示教师如何有效地组织教学。

本书可以作为高等院校有关专业专科生的教材和参考书，适合各单位网络管理员、网络工程技术人员以及广大网络爱好者阅读和参考。

本书由苏州市职业大学的谭方勇担任主编，他对本书的编写思路与大纲进行了总体策划，指导全书的编写工作；周莉、张燕担任副主编，肖长水、于复生、陆侃参编。谭方勇编写第 1 章、第 4 章、第 10 章、第 12 章以及附录，张燕编写第 3 章、第 5 章，周

莉编写第 8 章、第 9 章，肖长水编写第 6 章、第 7 章，陆侃编写第 11 章，于复生编写第 2 章。

由于时间仓促，书中难免存在不妥之处，敬请读者谅解，并提出宝贵意见。作者 E-mail 地址：tanfy@126.com。

作 者

2008 年 4 月

目　录

第 1 章　计算机网络安全概述及环境搭建

教学提示：本章主要从计算机网络安全的需求和现状的分析，引出计算机网络安全的必要性，并提出国内外对计算机网络安全的定义，以及网络安全的防御体系和相关的网络安全法规。另外，本章还将介绍网络安全实验平台的搭建。

教学要求：了解计算机网络安全的需求和现状，理解网络安全的定义和防御体系，掌握网络安全实验平台的搭建。

随着互联网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。近些年来，互联网在我国取得了突飞猛进的发展，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数量在不断的上升，如网络黑客攻击，计算机病毒、木马及蠕虫等字眼在我们眼前出现的概率也越来越大，因此，计算机网络安全问题必须得到重视，本章主要从计算机网络安全的需求和现状着手，提出网络安全的定义和安全防御体系结构，最后介绍在后续章节中要用到的实验环境的搭建。

1.1　计算机网络安全概述

1.1.1　网络安全的发展史

1. 网络安全问题的产生

计算机网络尤其是互联网具有较强的开放性、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，但是，也正由于它的这些特点随之带来很多安全问题，主要表现如下：

（1）信息泄露、信息污染及信息不可控等。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、社会以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、政府网站和国防通信设施等。

（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

网络安全问题也成为信息时代人类面临的巨大挑战。美国前总统克林顿在签发《保护信息系统国家计划》的总统咨文中陈述道："在不到一代人的时间里，信息革命以及计算机进入了社会的每一领域，这一现象改变了国家的经济运行和安全运作乃至人们的日常生活方式，然而，这种美好的、新的时代也带有它自身的风险。所有计算机驱动的系统都很容易受到侵犯和破坏。对重要的经济部门或政府机构的计算机进行任何有计划的攻击都可能产生灾难性的后果，这种危险是客观存在的。过去敌对力量和恐怖主义分子毫无例外地使用炸弹和子弹，现在他们可以把手提电脑变成有效武器，可以造成非常巨大的危害。如果人们想要继续享受信息时代的种种好处，继续使国家安全和经济繁荣得到保障，就必须保护计算机控制系统，使它们免受攻击。"

目前各种领域的计算机犯罪和网络侵权行为在数量、规模及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就达到几百亿美元，德国、英国也均在数十亿美元以上，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 20 秒就会发生一次网络入侵事件。我国的网络安全事件的发生率也在不断的上升，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，2007 年上半年我国发生的各类网络安全事件数大大超出了 2006 年，甚至有些事件超出了 2006 年全年该类事件的总和。如图 1-1 所示，为 2007 年上半年各类安全事件类型的分布图[①]。

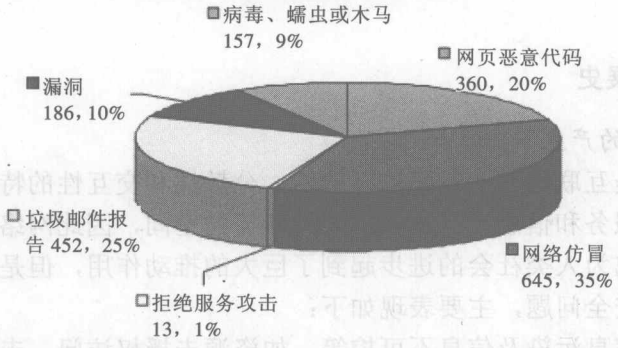


图 1-1　2007 年上半年网络安全事件类型分布

3. 网络安全的发展趋势

在互联网普及的同时，网络安全的威胁也在不断增加，并且黑客攻击技术与病毒技术相融合，所以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 CNCERT/CC 2007 年上半年网络安全工作报告。

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于好奇心重、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、网址嫁接及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。“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、木马攻击以及信息垃圾等。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、拒绝服务和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以及核心数据区，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。

1.1.2　网络安全的定义

网络安全是一门集计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论和信息论等多种学科于一体的综合性学科。

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，凡是涉及到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。

国际标准化组织（ISO）对计算机系统安全的定义是：“为数据处理系统建立和采用的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因遭到破坏、更改和泄露”。由此可以将计算机网络安全理解为：通过采用各种技术和管理措施，使网络系统正常运行，从而确保网络数据的可用性、完整性和保密性。所以，建立网络安全保护措施的目的是确保经过网络传输和交换的数据不会发生增加、修改、丢失和泄露等情况。

网络安全实际上主要包含以下几个方面：

（1）运行系统的安全，即要保证信息处理和传输系统的安全；

（2）网络上系统信息的安全；

（3）网络上信息传输的安全，即信息传输后果的安全；
（4）网络上信息内容的安全，即所谓狭义的“信息安全”。

1.1.3 网络安全的相关法规

要保证计算机网络的安全能得到保障，这不仅取决于在技术上的进步，还依赖社会法律、法规的完善。经过这些年的发展，许多国家都已经建立起了一套完善的安全法规，事实也证明它对网络的使用者起到了较好的约束作用，在一定程度上保证了计算机网络的安全。

西方发达国家，特别是美国和日本是计算机网络安全上的立法比较完善的国家，而一般的发展中国家和第三世界国家网络安全上的立法还不够完善。

在我国，政府对信息安全和网络安全问题非常重视，并积极推动网络安全管理和安全立法工作，目前网络安全方面的法规已经写入中华人民共和国宪法。于 1982 年 8 月 23 日写入中华人民共和国商标法，于 1984 年 3 月 12 日写入中华人民共和国专利法，于 1988 年 9 月 5 日写入中华人民共和国保守国家秘密法，于 1993 年 9 月 2 日写入中华人民共和国反不正当竞争法。近些年，我国还陆续颁布了《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国计算机信息网络国际联网管理暂行规定》、《计算机信息网络国际联网安全保护管理办法》、《中国互联网络域名注册暂行管理办法》、《中国互联网域名注册实施细则》等法规性文件，并在新刑法中明确了计算机犯罪与计算机违法行为的区别，从而为我国的网络安全管理提供了法律依据。

1.1.4 网络安全的评价标准

随着网络安全问题的日益严重，各个国家以及国际标准化组织制定了相应的协议和标准来加强计算机网络的安全。

1. 国际的评价标准

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。橙皮书的目标有三个：

（1）给计算机制造商提供一个标准，让其知道要符合可信度（特别是保护敏感数据）要求，他们的产品需要什么样的性能和特性；

（2）给国防部所属的部门一个衡量标准，他们可以根据此标准来评价一台计算机系统在处理保密信息和其他敏感数据方面的可信度；

（3）给其他特定的安全要求提供一个基础。

橙皮书把安全的级别从低到高分成 4 个类别：D 类、C 类、B 类和 A 类，每类又分几个级别，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 类安全等级最低，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，不受任何限制就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 类中有 C1 和 C2 两个安全子级，其中，C1 系统的可信计算基础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 级别应该具有访问控制环境（Controlled-access Environment）权利。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，如多次登录失败，也可以大致推测出可能有人想入侵系统。审计除了可以记录下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。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 级别的常见操作系统有：Unix、Novell 3.X 或者更高版本、Windows NT、Windows 2000 和 Windows Server 2003。

B 级中有三个级别，B1 级即标志安全保护（Labeled Security Protection），是支持多级安全（例如：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、绝密级别，这种安全级别的计算机系统一般在政府机构中，比如国防部和国家安全局的计算机系统。

B2 级，又称为结构保护级别（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，又叫做安全域级别（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、所有的安全特性。

设计必须从数学角度上进行验证，而且必须进行秘密通道和可信任分布分析。可信任分布（Trusted Distribution）的含义是：硬件和软件在物理传输过程中已经受到保护，以防止破坏安全系统。

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。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。在德国，德国信息技术安全局在 1989 年发表了自己的标准，同年，法国也发表了自己的标准“兰—白—红书”。

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

2. 国内的评价标准

在我国根据《计算机信息系统安全保护等级划分准则》，1999 年 10 月经过国家质量技术监督局批准发布准则将计算机安全保护划分为以下 5 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。这一个级别特别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。

1.2 网络安全威胁

无论是国内还是国外，网络安全受到威胁的程度在不断地恶化，如果不能得到有效的遏制，则对全球经济和社会发展的负面影响会越来越大。

1.2.1　网络安全威胁的来源

网络安全威胁的形式多种多样，有的可能很简单或者很笨拙，如密码尝试；有的可能很巧妙且很隐蔽地侵入公司内部网络进行非授权访问。网络安全威胁的来源一般来自于两类，即内部威胁和外部威胁。

1. 内部威胁

目前几乎绝大部分企业都比较重视来自企业网络外部的威胁，所有网络安全的开支也基本用于外部的安全防御，而内部威胁的防御却很少得到重视。美国知名咨询公司 Deloitte 在 2007 年的一项调查显示，在接受调查的 100 家跨国金融服务公司中，91%不知道如何应对来自内部员工的安全威胁。

实际上，网络内部的威胁对网络造成的影响与外部威胁一样，甚至更坏，因为网络内部用户具有更多有利条件，如他们具备一定的网络访问权限，熟悉企业的商业架构和网络体系结构，还可以方便地收集到有关网络操作、管理和安全实现上的相关信息，且可以利用这些信息来监视网络。所以，来自内部的威胁必须得到重视，否则可能会造成严重后果。

来自内部的威胁主要包括以下几个方面：

（1）错误使用和滥用关键、敏感数据和计算资源。无论是有不满情绪的员工的故意破坏，还是没有访问关键系统权限的员工因误操作而进入关键系统，由此而造成的数据泄露、偷窃、损坏或删除将给企业带来很大的负面影响。

（2）因不当使用 Internet 接入而降低生产率。不当使用 Internet 资源不但会浪费员工的时间，还会增加计算机网络的负担，降低了人员与网络的工作效率。

（3）如果工作人员发送、接收和查看攻击性材料，可能会形成敌意的工作环境，从而增大内耗。通常，对内部威胁的防御往往只能通过对内部员工的教育来解决，使之理解网络安全的重要性。如提示员工保管好自己的账号和密码，不要让别人使用，密码还需妥善保管且需定期更换。另外，还要警惕不要轻易打开外来的文件，而是先经过病毒扫描后再打开。

2. 外部威胁

外部威胁主要来自网络外部的入侵，这种入侵行为通常不易被发现，造成的影响也比较严重，而且当今来自外部的威胁也越来越多，发动这种攻击或入侵行为的可能来自网络外部的任何人，如黑客或者网络安全爱好者，因此对攻击的目的和来源也很难判断。

数据通信链路很容易进行接入窃听，因此它往往是不安全的，也很容易成为外部威胁的目标，如果与互联网相连，则最容易受到此类攻击。

对外部威胁的防范也有很多方法，可以对数据通信链路进行加密，例如，使用虚拟专用网（VPN）技术对不安全的通信链路进行加密传输，也可以通过设置访问控制列表（ACL）来限制某些通信数据等。

1.2.2 网络安全威胁的种类

计算机网络所面临的威胁一般可以分成两种：一是对网络中信息的威胁，二是对网络中设备的威胁。归结起来具体可以分成以下三类。

1. 非授权访问

非授权访问一般是没有事先经过同意，通过假冒、身份攻击及系统漏洞等手段来获取系统的访问权限，从而非法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

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，因此发动相对比较简单且具有越来越多的趋势，而且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

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。

1.3 网络安全防御体系

为了能够有效进行网络的安全防范，建立一套科学、可行的网络安全防御体系是非常有必要的。

1.3.1 网络安全防御体系的层次结构

一般可以把网络安全分为以下几个层次，即物理安全性、操作系统安全性、网络的安全性、应用安全性和管理安全性。

1. 物理安全性

物理安全也即物理环境的安全性，它包括通信线路的安全、物理设备的安全及机房的安全等。它主要涉及到：防火、防静电、防雷击、防电磁辐射和防盗等。例如，在机房内可配置 UPS 不间断电源，以保证停电时或异常情况下切换到由 UPS 供电，使计算机系统内存中的数据及程序不受影响。

2. 操作系统安全性

该层次的安全问题主要来自网络中主机上使用的操作系统的安全，如 Windows

NT/2000/XP/2003/Vista 系列、Linux/Unix 系列、Netware 以及其他专用操作系统。其安全主要包括操作系统的安全配置、操作系统的漏洞检测及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。

3. 网络的安全性

网络的安全问题一般是指网络信息的安全性，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的手段等手段。

4. 应用安全性

该层次的安全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、访问控制及数据库系统中数据的安全性等几方面。

5. 管理安全性

网络安全管理主要包括安全技术和设备的管理、安全管理制度及部门与人员的组织规则等。管理的制度化将对整个网络安全起着重要作用，严格的安全管理制度、明确的部门安全职责划分、合理的人员角色配置都可以在很大程度上降低其他层次的安全漏洞。

1.3.2　网络安全防御体系设计

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少。如图 1-2 所示，为一个网络安全防御体系的基本模型。

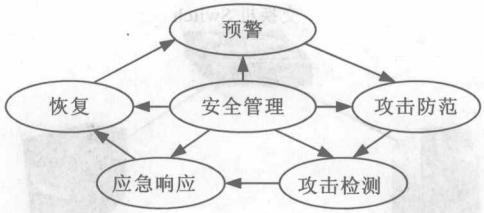


图 1-2　网络安全防御体系的基本模型

1.3.3　网络安全防御体系工作流程

1. 攻击前的防范

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，即进行日常的防御工作，也对事实的消息