项目 3 project 3

网络安全体系及管理

目前，世界各国高度重视网络安全，并上升为国家甚至全球发展战略。“没有网络安全就没有国家安全”成为共识，网络安全技术必须同管理密切结合，才能真正发挥实效。网络安全管理已经成为信息化建设和应用的首要任务，而且是一个涉及很多要素的系统工程，包括体系结构、法律、法规、政策、策略、规范、标准、机制、规划和措施等。

重点： 网络安全体系、法律、评估准则和方法，以及网络安全管理规范和制度。

难点： 网络安全评估准则和方法，以及网络安全管理规范、原则和制度，网络安全规划。

关键： 网络安全体系、法律、评估准则和方法，以及网络安全管理规范和制度。

目标： 理解网络空间安全战略意义，掌握网络安全体系、法律、评估准则和方法，理解网络安全管理规范、原则和制度，了解网络安全规划的主要内容和原则，掌握网络安全“统一威胁管理”实验。

教学视频
课程视频 3.1

3.1 项目分析 网络空间安全战略意义

【引导案例】 我国高度重视网络安全，已将其上升为国家战略。2014 年成立了中央网络安全和信息化领导小组，由中共中央总书记、国家主席、中央军委主席习近平亲自担任组长。2017 年正式实施的《中华人民共和国网络安全法》，为网络安全管理法制化奠定了极为重要的基础和保障。

3.1.1 网络空间安全战略及作用

1. 世界高度重视网络空间安全战略

【案例 3-1】 美国高度重视网络空间安全战略。美国将空军太空司令部（AFSPC）的网络责任转移给空战司令部（AFACC），并于 2018 年夏天开始承担网络空间安全责任。两个司令部已密切协调，调整战略角色和责任。美国空军部长海瑟·威尔逊

在声明中表示，此举将网络行动、情报、监视和侦察任务整合到同一司令部，从而有助于作战时加速决策制定过程。

美国空军太空司令部司令杰伊·雷蒙德表示，空军太空司令部将完全专注于保持“太空优势”。将网络行动和情报整合为同一司令部有助于提高作战能力，执行多域行动。威尔逊表示，美国国防战略加强美军信息获取和利用。美国空军参谋长戴维·戈德费恩表示，此举对“未来高端战斗”是必要的。

2. 各种网络攻击进一步增强

在各种网络攻击的整体防御上，用户通常采用具备大带宽储备和云服务防御方案等。随着 AI 设备与物联网的飞速发展，各种应用平台不断出现，其各种攻防将愈演愈烈。分布式拒绝服务（DDoS）等各种攻击将呈现出进一步增强、多样化、智能化的发展态势。

知识拓展 DDoS 将呈现多样化发展

【案例 3-2】 2018 年上半年国内外企事业机构的网络系统遭受 DDoS 攻击更为严重。无论从网络数据流量还是攻击次数和攻击强度方面都有新的上升。DDoS 黑色产业链的人员与技术的发展降低了整体入门的门槛，在溯源监控中发现，有的 DDoS 黑客团伙的平均年龄 20 岁左右，甚至有未满 16 岁的学生也加入 DDoS 黑客团伙。

3. 网络安全防范意识和能力不足

很多专家表示，网络安全问题已经达到非常严重的程度，如果再不采取措施，经济会遭受重大损失。德国研究员 Zinaida Benenson 对恶意链接的调查显示：20%的人会单击陌生邮件中的链接，40%的人因好奇心会单击社交网络链接。国内机构对重大网络安全事件关注度调查显示：有 40.4%的网民会持续关注相关内容，担心自己受攻击，想了解防御方法；26.7%的网民会关注相关内容，但感觉不太会受影响；13.9%的网民看过报道，但不怎么关心，感觉和个人关系不大；19.0%的网民完全不了解、不知道近期发生的重大网络安全事件。统计显示，82.6%的网民都没有接受过任何形式的网络安全培训；13%的网民只接受过很少的专门培训；仅 4.4%的网民接受过专门培训。

知识拓展 网络安全意识调研情况

2019 年 9 月 15 日“网民网络安全感满意度调查报告”发布，我国网民认为网络安全的占 51.25%，比 2018 年提升 12.91%；网民安全感满意度指数为 69.128 分（满分为 100 分）。另据统计，2016 年网民因个人信息泄露等原因一年经济损失高达 915 亿元。

3.1.2 网络安全管理是关键

进入21世纪现代信息化社会，随着各种网络技术的快速发展和广泛应用，出现了很多网络安全问题，致使网络安全技术的重要性更加突出，**网络安全已经成为各国关注的焦点**，不仅关系到机构和个人用户的信息资源和资产风险，也关系到国家安全和社会稳定，已成为热门研究和人才需求的新领域。网络空间已经逐步发展成为继陆、海、空、天之后的第五大战略空间，是影响国家安全、社会稳定、经济发展与文化传播的**核心、关键和基础**。

【案例3-3】 网络安全已经成为信息时代国家安全的战略。同时网络安全已经成为世界热门研究课题之一，并引起社会广泛关注。网络安全是个系统工程，已经成为世界各国战略优势激烈竞争、现代信息化建设、社会稳定发展和广泛应用的首要任务。

知识拓展
网络安全的重要战略性

我国极为重视网络安全工作，充分认识到网络安全的战略意义。在日常网络安全工作中必须坚持网络安全管理和相关技术的紧密结合，“七分管理，三分技术，运作贯穿始终”，管理是关键，技术是保障，实际上网络安全技术也包含很多策略、机制、设置、标准、规范及防范对策等管理技术。

☺讨论思考

（1）举例说明网络安全管理的教训和启示。

（2）举例说明网络安全管理的重大意义。

教学视频
课程视频3.2

3.2 任务1 网络安全体系结构

3.2.1 目标要求

本任务主要学习目标的具体要求如下。

（1）掌握OSI网络安全体系结构和TCP/IP网络安全管理体系结构。

（2）掌握网络安全攻防体系结构和网络空间安全学科知识体系。

（3）理解网络安全保障体系和保障体系总体框架。

（4）了解可信计算网络安全防护体系及应用。

3.2.2 知识要点

1. OSI 网络安全体系结构

国际标准化组织(ISO)提出的开放系统互连(OSI)参考模型，主要用于进行异构网络及设备互连的开放式层次结构的研究。OSI 网络安全体系结构包括网络安全机制和网络安全服务。

(1) 网络安全机制。ISO 7498-2《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、鉴别交换机制、信息量填充机制、路由控制机制和公证机制。

(2) 网络安全服务。**网络安全服务的内容**主要有 5 项：鉴别服务、访问控制服务、数据保密性服务、数据完整性服务和可审查性服务。

知识拓展
网络安全服务的主要内容

2. TCP/IP 网络安全管理体系结构

TCP/IP **网络安全管理体系结构**如图 3-1 所示，包括 3 方面：分层安全管理、安全服务与机制、系统安全管理。有机地综合了安全管理、技术和机制各方面，对网络安全整体管理与实施和效能的充分发挥起到至关重要的作用。

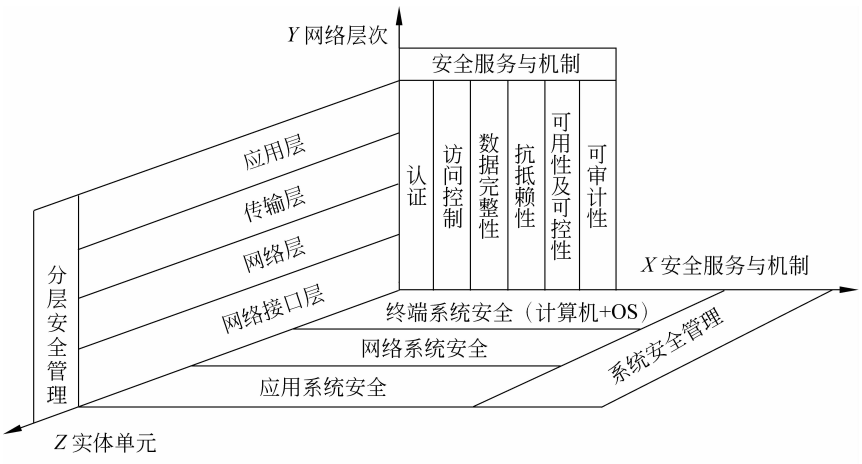

图 3-1 TCP/IP 网络安全管理体系结构

3. 网络安全攻防体系结构

网络安全攻防体系结构主要包括两大方面：攻击技术和防御技术。知其攻击才能有针对性地进行防御，主要的网络安全攻防体系结构如图 3-2 所示。

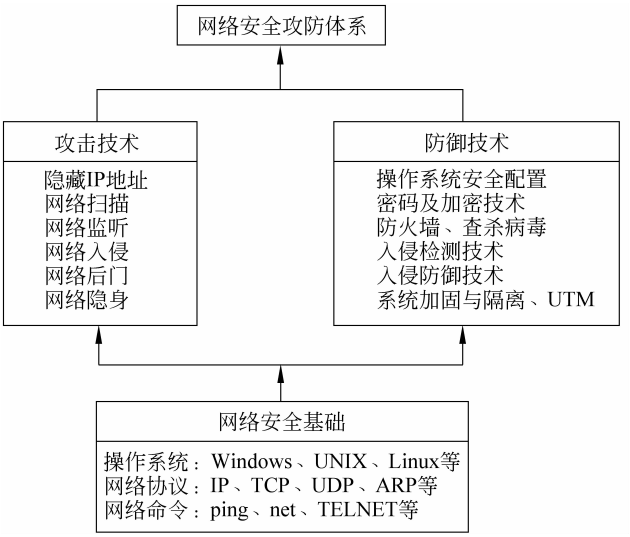

图 3-2　网络安全攻防体系结构

为了更有效地进行网络安全防范，需要“知己知彼，百战不殆”，掌握好网络安全攻防体系结构、常见的攻击技术和手段。主要常见的网络攻击技术包括 6 种：隐藏 IP 地址、网络扫描、网络监听、网络入侵、网络后门、网络隐身。

知识拓展　主要常见的网络攻击技术

主要的网络防御技术包括操作系统安全配置、密码及加密技术、防火墙、查杀病毒、入侵检测技术、入侵防御技术、系统加固与隔离、统一威胁资源管理（UTM）等。

知识拓展　网络安全防御常用技术

4. 网络空间安全学科知识体系

教育部高等学校信息安全教学指导委员会副主任委员、上海交通大学网络空间安全学院院长李建华教授，2018 年在“第十二届中国网络空间安全学科专业建设与人才培养研讨会”上“新工科背景下多元化网络空间安全人才培养及学科建设创新”报告中提出网络空间安全学科知识体系，如图 3-3 所示。

由于网络空间安全的威胁和隐患剧增，急需构建新型网络空间安全防御体系，并从传统线性防御体系向新型多层次的立体式网络空间防御体系发展。以相关法律、准则、策略、机制和技术为基础，以安全管理及运行防御体系贯彻始终，从第一层物理层防御体系、第二层网络层防御体系到第三层系统层与应用层防御体系构成新型网络空间安全防御体系，可以实现多层防御的立体化安全区域，将网络空间中的结点分布于所有域中，其中的所有活动支撑着其他域中的活动，且其他域中的活动同样可以对网络空间产生影响。构建的这种网络空间安全立体防御体系如图 3-4 所示。

特别理解　网络空间安全基本含义

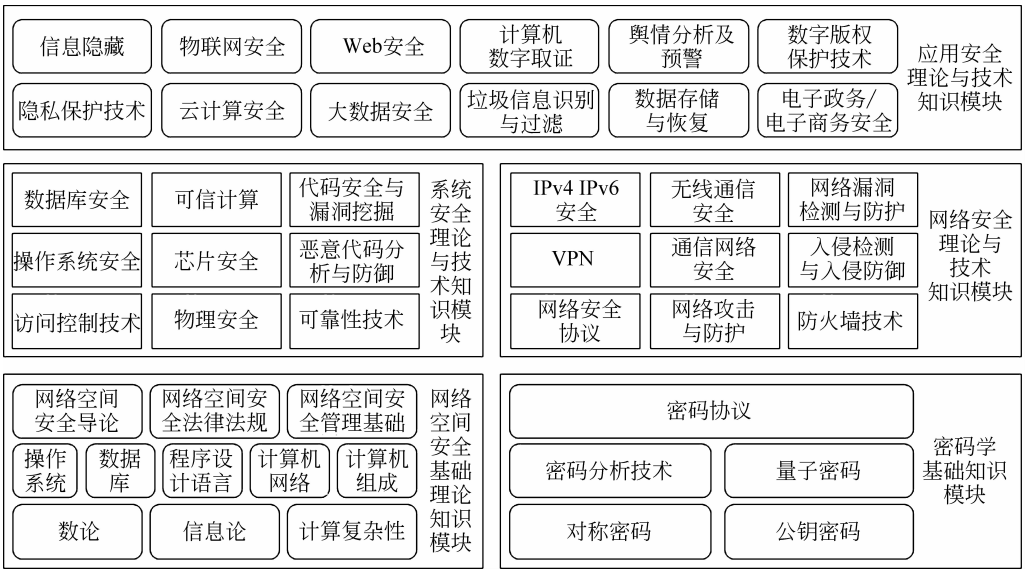

图 3-3 网络空间安全学科知识体系

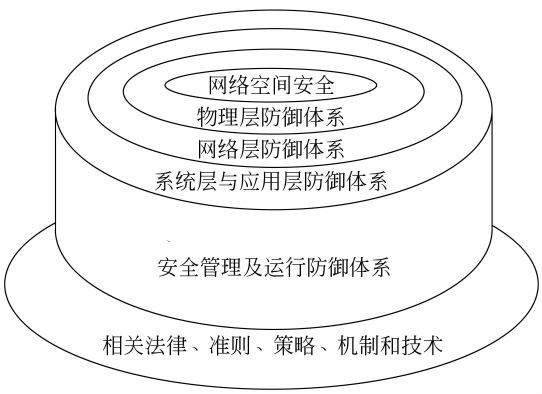

图 3-4 网络空间安全立体防御体系

5. 网络安全保障体系

网络安全保障体系如图 3-5 所示。其保障功能主要体现在对整个网络系统的风险及隐患进行及时评估、识别、控制和应急处理等，便于有效地预防、保护、响应与恢复，确保系统安全运行。

(1) 网络安全保障关键要素。主要包括 4 方面：网络安全策略、网络安全管理、网络安全运作和网络安全技术，如图 3-6 所示。其中，网络安全策略为网络安全保障的核心，主要包括网络安全的战略、政策和标准；网络安全管理是机构的管理行为，主要包括安全意识、组织结构和审计监督；网络安全运作是日常管理行为，包括运作流程和对象管理；网络安全技术是网络系统的行为，包括安全服务、措施和基础设施。

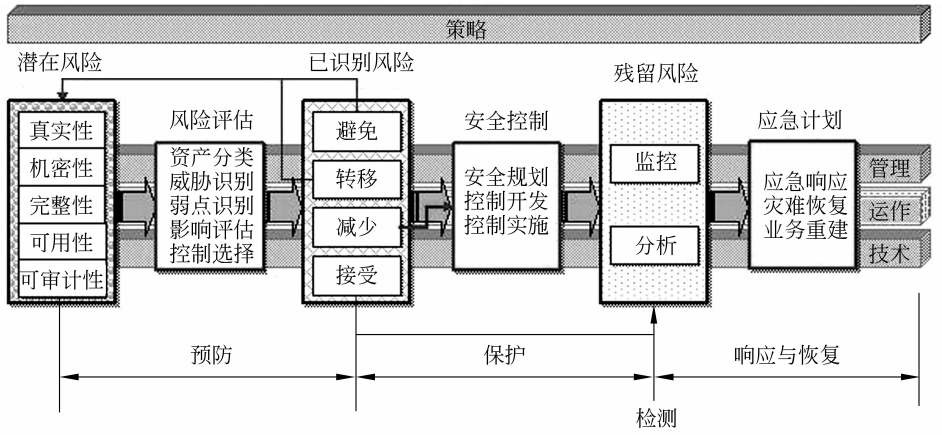

图 3-5　网络安全保障体系

知识拓展
P2DR 模型的优缺点

P2DR 模型是美国 ISS 公司提出的动态网络安全体系的代表模型，包含 4 个主要部分：安全策略（policy）、防护（protection）、检测（detection）和响应（response），如图 3-7 所示。

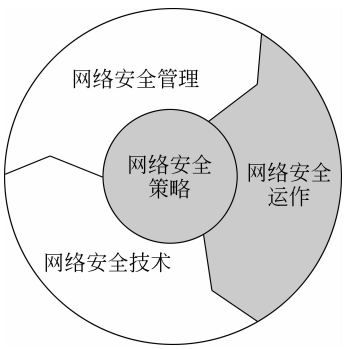

图 3-6　网络安全保障要素

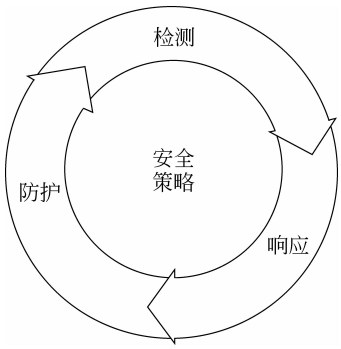

图 3-7　P2DR 模型示意图

（2）网络安全保障总体框架。面对网络系统的各种威胁和风险，以往针对单方面具体的安全隐患所提出的具体解决方案具有一定的局限性，应对的措施也难免顾此失彼。面对新的网络环境和威胁，需要建立一个以深度防御为特点的网络安全保障体系。

特别理解
网络安全风险管理内涵

对于企事业机构，常用的**网络安全保障体系总体框架**如图 3-8 所示。此保障体系的外围主要包括风险管理、法律法规、标准符合性。

知识拓展
网络安全保障体系架构

网络安全管理的本质是对网络信息安全风险进行动态及有效管理和控制。风险管理是网络运营管理的核心，风险分为信用风险、市场风险和操作风险，其中包括网络安全风险。在网络安全保障体系总体框架中，充分体现了风险管理的理念。

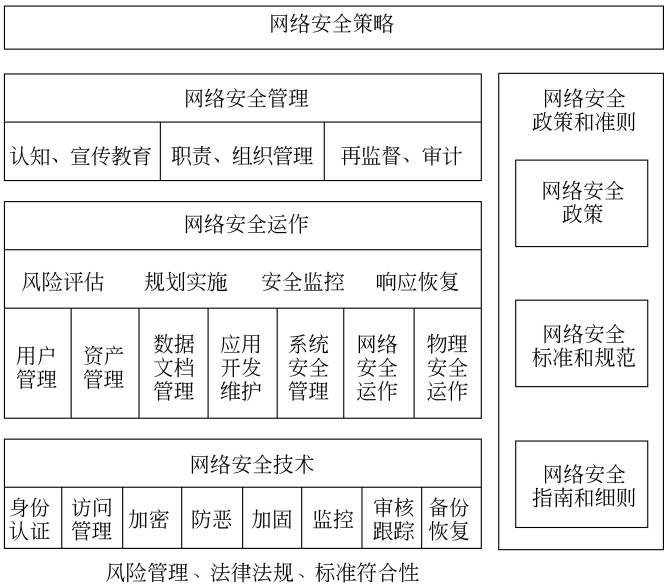

图 3-8 网络安全保障体系总体框架

6. 可信计算网络安全防护体系

沈昌祥院士强调：可信计算是网络空间战略最核心技术之一，要坚持“五可”“一有”的技术路线。可信计算网络安全防护体系（即“五可”）包括以下几方面：一是可知，对全部的开源系统及代码完全掌握其细节；二是可编，完全理解开源代码并可自主编写；三是可重构，面向具体的应用场景和安全需求，对基于开源技术的代码进行重构，形成定制化的新体系结构；四是可信，通过可信计算技术增强自主操作系统免疫性，防范自主系统中的漏洞影响系统安全性；五是可用，做好应用程序与操作系统的适配工作，确保自主操作系统能够替代国外产品。“一有”是对最终的操作系统拥有自主知识产权，并处理好所使用的开源技术的知识产权问题。

知识拓展
开源技术及其纵深防御

☺讨论思考

（1）OSI 网络安全体系结构主要有哪些？

（2）画出 TCP/IP 网络安全管理体系结构图。

（3）概述网络安全保障体系和保障体系总体框架。

3.3 任务 2 网络安全相关法律法规

教学视频
课程视频 3.3

3.3.1 目标要求

本任务主要学习目标的具体要求如下。

（1）了解国外网络安全的法律法规。

（2）掌握我国网络安全的法律法规。

3.3.2 知识要点

现代信息化社会各种信息技术发展与更新很快，但在全球广泛应用的时间却较短，具体的法律法规在较短的时期内不可能十分完善，正随着信息化社会不断发展而完善。

1. 国外网络安全的法律法规

1）国际合作立法打击网络犯罪

自20世纪90年代以来，很多国家为了更有效打击利用计算机网络进行的各种违法犯罪活动，都强化了法律手段，欧盟已成为在刑事领域做出国际示范的典型，分别于2000年两次颁布《网络刑事公约（草案）》，现已有43个国家借鉴了这一公约草案。在不同国家的刑事立法中，印度的相关做法具有一定代表性，于2000年6月颁布了《信息技术法》，制定出一部规范网络安全的基本法。一些国家修订了原有的刑法，以适应保障计算机网络安全的需要。如美国2000年修订了以前的《计算机反欺诈与滥用法》，增加了法人犯罪的责任，补充了类似规定。

2）禁止破坏数字化技术保护措施的法律

1996年12月，世界知识产权组织做出了“禁止擅自破解他人数字化技术保护措施”的规定，以此作为保障网络安全的一项主要内容进行规范。现在，欧盟成员国、日本、美国等大多数国家都将其作为一种网络安全保护规定，纳入本国的法律之中。

3）与“入世”有关的网络法律

1996年12月在联合国第51次大会通过了联合国贸易法委员会的《电子商务示范法》，对于网络市场中数据电文、网上合同成立及生效的条件、传输等专项领域的电子商务等，都做了十分明确具体的规定。1998年7月新加坡的《电子交易法》出台。1999年12月，世贸组织西雅图外交会议上，制定电子商务规范成为一个主要议题。

4）其他相关立法

很多国家除了制定保障网络健康发展的法律法规以外，还专门制定了综合性的、原则性的网络基本法。如韩国2000年修订的《信息通信网络利用促进法》，其中包括对“信息网络标准化”和实名制的规定，对成立“韩国信息通信振兴协会”等民间自律组织的规定等。在印度，政府机构成立了“网络事件裁判所”，以解决影响网络安全的民事纠纷。

5）民间管理、行业自律及道德规范

世界各国在规范网络使用行为方面都很注重发挥民间组织的作用，特别是行业自律作用。德国、英国、澳大利亚等学校中网络使用的“行业规范”十分严格。澳大利亚每周都要求教师填写一份保证书，申明不从网上下载违法内容。德国的网络用户一旦有校方规定禁止的行为，服务器立即会发出警告。慕尼黑大学、明斯特大学等院校都制定了《关于数据处理与信息技术设备使用管理办法》，要求严格遵守。

2. 国内网络安全的法律法规

【案例 3-4】《中华人民共和国网络安全法》为网络安全工作提供切实法律保障。全国人民代表大会常务委员会于 2016 年 11 月发布了《中华人民共和国网络安全法》，这是我国第一部全面规范网络空间安全管理方面问题的基础性法律，是我国网络空间法治建设的重要里程碑，是依法治网、化解网络风险的法律重器，是让互联网在法治轨道上健康运行的重要保障。

知识拓展
网络安全的法治化管理

我国从依法治理网络安全的实际需要出发，国家及相关部门、行业和地方政府都相继制定并颁布了很多有关网络安全的法律法规。

我国网络安全立法体系分为以下 3 个层次。

（1）法律。全国人民代表大会及其常委会通过的法律规范。我国与网络安全相关的法律主要有《中华人民共和国宪法》《中华人民共和国刑法》《中华人民共和国治安管理处罚条例》《中华人民共和国刑事诉讼法》《中华人民共和国国家安全法》《中华人民共和国保守国家秘密法》《中华人民共和国网络安全法》《中华人民共和国行政处罚法》《中华人民共和国行政诉讼法》《全国人大常委会关于维护互联网安全的决定》《中华人民共和国人民警察法》等。

（2）行政法规。主要指国务院为执行宪法和法律而制定的法律规范。与网络信息安全有关的行政法规包括《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》《商用密码管理条例》《中华人民共和国电信条例》《互联网信息服务管理办法》《计算机软件保护条例》等。

（3）地方性法规、规章、规范性文件。主要指国务院各部委根据法律和国务院行政法规与法律规范，以及省、自治区、直辖市和较大的市人民政府根据法律、行政法规和本省、自治区、直辖市的地方性法规制定的法律规范性文件。

公安部制定了《计算机信息系统安全专用产品检测和销售许可证管理办法》《计算机病毒防治管理办法》《金融机构计算机信息系统安全保护工作暂行规定》和有关安全员培训要求等。

工业和信息化部制定了《互联网电子公告服务管理规定》《软件产品管理办法》《计算机信息系统集成资质管理办法》《国际通信出入口局管理办法》《国际通信设施建设管理规定》《中国互联网络域名管理办法》《电信网间互联管理暂行规定》等。

☺讨论思考

（1）国外网络安全的法律法规有哪些？

（2）概述我国网络安全立法体系。

3.4 任务3 网络安全评估准则和测评方法

3.4.1 目标要求

本任务主要学习目标的具体要求如下。

（1）了解国外网络安全主要评估标准及准则。
（2）掌握国内网络安全评估准则及系统安全保护等级划分。
（3）理解网络安全主要的测评种类和方法。

3.4.2 知识要点

网络安全标准是确保网络信息安全的产品和系统在设计研发、生产建设、使用、测评和管理维护过程中，解决产品和系统的一致性、可靠性、可控性、先进性和符合性的技术规范和依据。网络安全标准是各国信息安全保障体系的重要组成部分，是政府进行宏观管理的重要手段。

1. 国外网络安全评估标准

国际性标准化组织主要包括国际标准化组织（ISO）、国际电工委员会（IEC）及国际电信联盟（ITU）所属的电信标准化组织（ITU-TS）等。ISO是总体标准化组织，而IEC在电工与电子技术领域里相当于ISO的位置。1987年，ISO和IEC成立了联合技术委员会（JTC1）。ITU-TS则是一个联合缔约组织。这些组织在安全需求服务分析指导、安全技术研制开发、安全评估标准等方面制定了一些标准草案。

知识拓展
其他国际组织的安全标准

1）美国TCSEC

1983年由美国国防部制定了**可信计算系统评价准则**（Trusted Computer Standards Evaluation Criteria，TCSEC），即网络安全**橙皮书或橘皮书**，主要利用计算机安全级别评价计算机系统的安全性。它将安全分为4方面（类别）：安全政策、可说明性、安全保障和文档。将这4方面（类别）又分为7个安全级别，从低到高依次为D、C1、C2、B1、B2、B3和A级。1985年，TCSEC成为美国国防部的标准，后来基本没有更改，一直是评估多用户主机和小型操作系统的主要方法。

数据库系统和网络其他子系统也一直利用橙皮书进行评估。TCSEC将安全级别从低到高分成4个类别：D类、C类、B类和A类，并分为7个级别，如表3-1所示。

通常，安全级别设计需要从数学角度上进行验证，而且必须进行秘密通道分析和可信任分布分析。

表 3-1 安全级别分类

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

2) 美国联邦准则

美国联邦准则(FC)参照了加拿大的评价标准 CTCPEC 与网络安全 TCSEC,目的是提供网络安全 TCSEC 的升级版本,同时保护已有的网络建设和投资。FC 是一个过渡标准,之后结合 ITSEC 发展为联合公共准则。

3) 欧洲 ITSEC

信息技术安全评估标准(Information Technology Security Evaluation Criteria,ITSEC),俗称欧洲的白皮书,将保密作为安全增强功能,仅限于阐述技术安全要求,并未将保密措施直接与计算机功能相结合。ITSEC 是欧洲的英国、法国、德国和荷兰 4 国在借鉴橙皮书的基础上于 1989 年联合提出的。橙皮书将保密作为安全重点,而 ITSEC 则将首次提出的完整性、可用性与保密性作为同等重要的因素,并将可信计算机的概念提高到可信信息技术的高度。ITSEC 定义了从 E0 级(不满足品质)到 E6 级(形式化验证)的 7 个安全等级,对于每个系统安全功能可分别定义。ITSEC 预定义了 10 种功能,其中前 5 种与橘皮书中的 C1～B3 级基本类似。

4) 通用评估准则

通用评估准则(Common Criteria for IT Security Evaluation,CC)由美国等国家与国际标准化组织联合提出,并结合 FC 及 ITSEC 的主要特征,强调将网络信息安全的功能与保障分离,将功能需求分为 9 类 63 族(项),将保障分为 7 类 29 族。CC 的先进性体现在其结构的开放性、表达方式的通用性,以及结构及表达方式的内在完备性和实用性 4 方面。CC 于 1996 年发布第一版,充分结合并替代了 ITSEC、TCSEC、FC 等国际上重要的信息安全评估标准而成为通用评估准则,并历经了很多更新和改进。CC 主要确定评估信息技术产品和系统安全性的基本准则,提出国际公认的表述信息技术安全性的结构,将安全要求分为规范产品和系统安全行为的功能要求,以及解决正确有效地实施其功能的保证要求。中国测评中心常采用此准则进行测评。

5) ISO 安全体系结构标准

开放系统标准建立框架的依据是国际标准 ISO 7498-2—1989《信息处理系统开放系统互连基本参考模型 第 2 部分:安全体系结构》,给出网络安全服务与有关机制的基本描述,确定在参考模型内部可提供的服务与机制。此标准从体系结构的角度描述 ISO 基

本参考模型之间的网络安全通信所提供的网络安全服务和网络安全机制，并说明了网络安全服务及其相应机制在安全体系结构中的关系，建立了 OSI 的网络安全体系结构框架。并在身份认证、访问控制、数据加密、数据完整性和防止抵赖方面提供了 5 种网络安全服务，如表 3-2 所示。

表 3-2　ISO 提供的网络安全服务

服　　务	用　　途
身份验证	身份验证是证明用户及服务器身份的过程
访问控制	用户身份一经过验证就发生访问控制，这个过程决定用户可以使用、浏览或改变哪些系统资源
数据加密	这项服务通常使用加密技术保护数据免于未授权的泄露，可避免被动威胁
数据完整性	这项服务通过检验或维护信息的一致性，避免主动威胁
防止抵赖	抵赖是指否认曾参加全部或部分事务的能力，防止抵赖服务提供关于服务、过程或部分信息的起源证明或发送证明

目前，国际上通用的网络与信息安全相关标准主要可分为三大类，如图 3-9 所示。

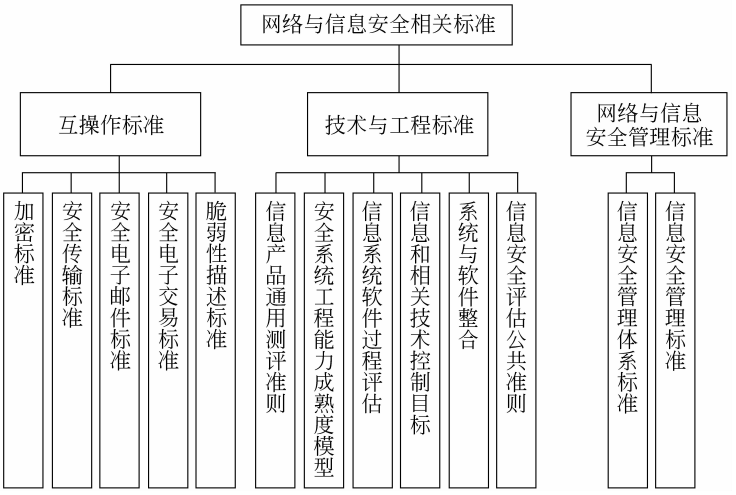

图 3-9　网络与信息安全相关标准

2. 国内网络安全评估准则

1）系统安全保护等级划分准则

1999 年 10 月经国家质量技术监督局批准发布的《计算机信息系统安全保护等级划分准则》，主要依据 GB 17859—1999《计算机信息系统安全保护等级划分准则》和 GA 163—1997《计算机信息系统安全专用产品分类原则》，将计算机系统安全保护划分为 5 个级别，如表 3-3 所示。

表 3-3 我国计算机系统安全保护等级划分

等级	名 称	具体描述
第一级	用户自我保护级	安全保护机制可以使用户具备安全保护的能力，保护用户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，使所有用户对自身行为的合法性负责
第三级	安全标记保护级	除具备前一级所有的安全保护功能外，还要求以访问对象标记的安全级别限制访问者的权限，实现对访问对象的强制访问
第四级	结构化保护级	除具备前一级所有的安全保护功能外，还将安全保护机制划分为关键部分和非关键部分，对关键部分可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	除具备前一级所有的安全保护功能外，还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

最近十几年，我国提出的有关信息安全实施等级保护问题，经过专家多次反复论证研究，其相关制度得到不断细化和完善。

知识拓展 完善信息安全保护等级

*2）我国网络信息安全标准化现状

在中国的信息安全标准化建设方面，主要按照国务院授权，在国家质量监督检验检疫总局管理下，由国家标准化管理委员会统一管理全国标准化工作，该委员会下设 255 个专业技术委员会。中国标准化工作实行统一管理与分工负责相结合的管理体制，由 88 个国务院有关行政主管部门和国务院授权的有关行业协会分工管理本部门、本行业的标准化工作，由 31 个省、自治区、直辖市政府有关行政主管部门分工管理本行政区域内、本行业的标准化工作。1984 年成立了全国信息技术安全标准化技术委员会(CITS)，在国家标准化管理委员会及工业和信息化部的共同领导下负责全国信息技术领域和与 ISO/IEC JTC1 对应的标准化工作，下设 24 个分技术委员会和特别工作组，主要从事国内外对应的标准化工作。

知识拓展 我国网络信息安全的标准化概况

3. 网络安全的测评方法

通过对网络系统进行全面、彻底、有效的安全测评，可查找并分析出网络安全漏洞、隐患和风险，以便采取措施提高系统防御及抗攻击能力。根据网络安全评估结果、业务的安全需求、安全策略和安全目标，提出合理的安全防护措施建议和解决方案。具体测评可通过网络安全管理的计划、规划、设计、策略和技术措施等方面进行。

1）测评目的和方法

(1) 网络安全的测评目的。网络安全测评目的包括如下内容。

① 搞清机构具体信息资产的实际价值及状况。

② 确定机构网络资源的机密性、完整性、可用性、可控性和可审查性的威胁风险及程度。

③ 通过调研分析，搞清当前机构网络系统实际存在的具体漏洞隐患及状况。

④ 明确与该机构信息资产有关的风险和具体需要改进之处。

⑤ 提出改变现状具体建议和方案，将风险降低到可接受的水平。

⑥ 为构建合适的安全计划和策略做好准备。

(2) 网络安全常用测评类型。网络安全**通用的测评类型**分为5个。

① 系统级漏洞测评。主要检测系统漏洞、系统安全隐患和基本安全策略及状况。

② 网络级风险测评。主要测评相关的所有网络及基础设施的风险范围。

③ 机构的风险测评。对整个机构进行整体风险分析，分析对其信息资产的具体威胁和隐患，分析处理信息漏洞和隐患，对实体系统及运行环境的各种信息进行检验。

④ 实际入侵测试。对具有成熟系统安全程序的机构进行检验，以测评该机构对具体模式的网络入侵的实际反应能力。

⑤ 审计。深入实际检查具体的安全策略和记录情况以及该组织具体执行的情况。

(3) 调研及测评方法。调研和测评时，收集的信息主要有3种基本信息源：调研对象、文本查阅和物理检验。调研对象主要是与现有系统安全和组织实施相关的人员，重点是熟悉情况的人员和管理者。为了准确测评所保护的信息资源及资产，调研提纲尽量简单易懂，且所提供的信息与调研人员无直接利害关系，同时审查现有的安全策略及关键的配置情况，包括已经完成和正在草拟或修改的文本。还应收集对该机构的各种设施的审查信息。

2) 测评标准和内容

(1) 测评前提。在网络安全实际测评前，应重点考察3方面的测评因素：服务器和终端及其网络设备安装区域环境的安全性；设备和设施的质量安全可靠性；外部运行环境及内部运行环境相对安全性。

(2) 测评依据和标准。主要根据ISO或国家有关的通用评估准则、《信息安全技术评估通用准则》《计算机信息系统安全保护等级划分准则》和《信息安全等级保护管理办法(试行)》等作为评估标准。经过各方认真研究和讨论达成的相关标准及协议也可作为网络安全测评的重要依据。

(3) 测评内容。对网络安全的评估内容主要包括安全策略测评、网络实体(物理)安全测评、网络体系安全测评、安全服务测评、病毒防护安全性测评、审计安全性测评、备份安全性测评、紧急事件响应测评和安全组织与管理测评等。

3) 网络安全策略测评

(1) 测评事项。利用网络系统规划及设计文档、安全需求分析文档、网络安全风险测评文档和网络安全目标，测评网络安全策略的有效性。

(2) 测评方法。采用专家分析的方法，主要测评安全策略实施及效果，包括安全需求是否满足、安全目标是否能够实现、安全策略是否有效、实现是否容易、是否符合安全设计原则、各安全策略是否一致等。

(3) 测评结论。依据测评的具体结果，对比网络安全策略的完整性、准确性和一致性。

4) 网络实体安全测评

(1) 测评项目。包括以下内容：网络基础设施、配电系统；服务器、交换机、路由器、

配线柜、主机房；工作站、工作间；记录媒体及运行环境。

（2）测评方法。采用专家分析法，主要测评对物理访问控制（包括安全隔离、门禁控制、访问权限和时限、访问登记等）、安全防护措施（防盗、防水、防火、防震等）、备份（安全恢复中需要的重要部件的备份）及运行环境等的要求是否实现、是否满足安全需求。

（3）测评结论。依据实际测评结果，确定网络系统的实际实体安全及运行环境情况。

5）网络体系的安全性测评

知识拓展 网络体系的安全性测评

6）安全服务的测评

（1）测评项目。主要包括认证、授权、数据安全性（保密性、完整性、可用性、可控性、可审查性）、逻辑访问控制等。

（2）测评方法。采用扫描检测等工具截获数据包，分析上述各项是否满足安全需求情况。

（3）测评结论。依据测评结果，表述安全服务的充分性和有效性。

7）病毒防护安全性测评

（1）测评项目。主要检测服务器、工作站和网络系统是否配备了有效的防病毒软件及病毒清查的执行情况。

（2）测评方法。主要利用专家分析和模拟测评等测评方法。

（3）测评结论。依据测评结果，表述计算机病毒防范实际情况。

8）审计的安全性测评

（1）测评项目。主要包括审计数据的生成方式安全性、数据充分性、存储安全性、访问安全性及防篡改的安全性。

（2）测评方法。主要采用专家分析和模拟测试等测评方法。

（3）测评结论。依据测评具体结果表述审计的安全性。

9）备份的安全性测评

（1）测评项目。主要包括备份方式、方法、存储的安全性和访问控制情况等。

（2）测评方法。采用专家分析的方法，依据安全需求、业务计划，测评备份的安全性情况。

（3）测评结论。依据测评结果，表述备份系统的安全性。

10）紧急事件响应测评

（1）测评项目。主要包括紧急事件响应程序及其有效应急处理情况，以及平时的应急准备情况。

（2）测评方法。模拟紧急事件响应条件，检测响应程序是否有序且有效地处理安全事件。

（3）测评结论。依据实际测评结果，对紧急事件响应程序和应急预案及措施的充分性、有效性进行评价。

知识拓展 网络安全组织和管理测评

11）网络安全组织和管理测评

☺讨论思考

（1）国外网络安全主要的评估标准及准则有哪些？

（2）简述国内网络安全评估准则及系统安全保护等级。

（3）举例说明一种网络安全的测评种类和方法。

3.5 项目案例 网络安全管理工具应用

网络安全管理员在网络安全检测与安全管理过程中，经常在“开始”菜单的“运行”（新版本为“搜索文件或程序”）栏内输入 cmd（运行 cmd.exe），然后，在 DOS 环境下使用一些网络管理工具和命令方式，直接进行查看和检测网络有关信息。

3.5.1 目标要求

本任务主要学习目标的具体要求如下。

（1）熟悉网络连通检测及端口扫描工具的使用方法。

（2）掌握显示网络配置信息与设置及连接监听端口的方法。

（3）学会查询、删除、修改用户信息应用及创建任务命令操作。

3.5.2 知识要点

1. 网络连通检测及端口扫描

1）ping 命令

ping 命令的主要功能是通过发送 Internet 控制报文协议 ICMP 包，检验与另一台 TCP/IP 主机的 IP 级连通情况。网络管理员常用这个命令检测网络的连通性和可到达性。同时，可将应答消息的接收情况和往返过程的次数一起进行显示。

【案例 3-5】 如果只使用不带参数的 ping 命令，窗口将会显示命令及其各种参数使用的帮助信息，如图 3-10 所示。使用 ping 命令的语法格式是“ping＋对方计算机名或者 IP 地址”。如果连通的话，返回的连通提示信息如图 3-11 所示。

2）quickping 命令和其他命令

quickping 命令可以快速探测网络中运行的所有主机情况。也可以使用跟踪网络路由程序 Tracert 命令、TraceRoute 程序和 Whois 程序进行端口扫描检测与探测，还可以利用网络扫描工具软件进行端口扫描检测，常用的网络扫描工具包括 SATAN、NSS、Strobe、Superscan 和 SNMP 等。

2. 显示网络配置信息及设置

ipconfig 命令的主要功能是显示所有 TCP/IP 网络配置信息、刷新动态主机配置协

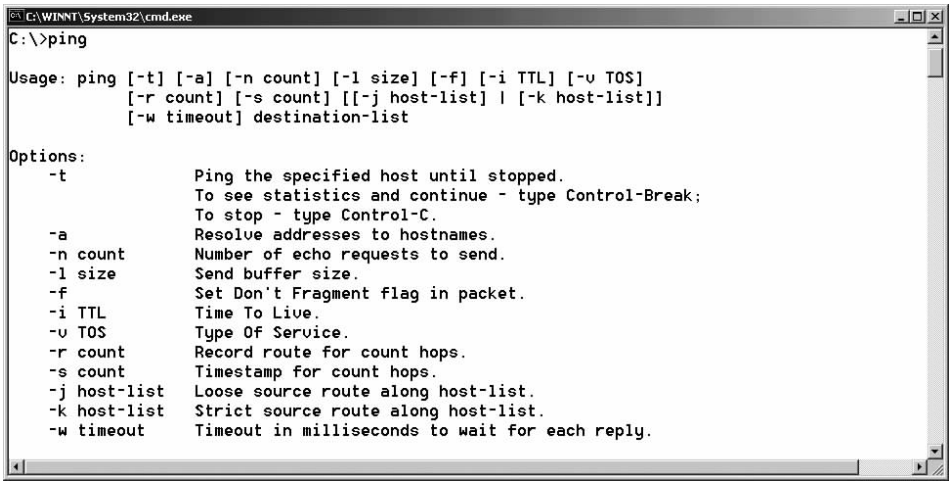

图 3-10 使用 ping 命令的提示信息

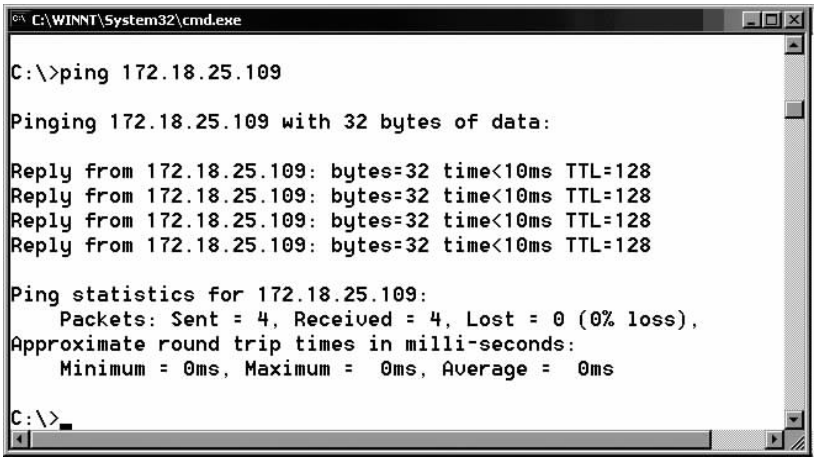

图 3-11 利用 ping 命令检测网络的连通性

议(dynamic host configuration protocol,DHCP)和域名系统(DNS)设置。

【案例 3-6】 如果使用不带参数的 ipconfig,可以显示所有网络适配器(网卡)的 IP 地址、子网掩码和默认网关。在 DOS 命令行下输入 ipconfig 命令可以出现有关提示信息,如图 3-12 所示。

利用 ipconfig /all 命令可以查看所有完整的 TCP/IP 配置信息。对于具有自动获取 IP 地址的网卡,则可以利用 ipconfig /renew 命令更新 DHCP 的配置。

3. 显示连接监听端口方法

netstat 命令的主要功能:显示活动的连接、监听端口、以太网统计信息、IP 路由表、

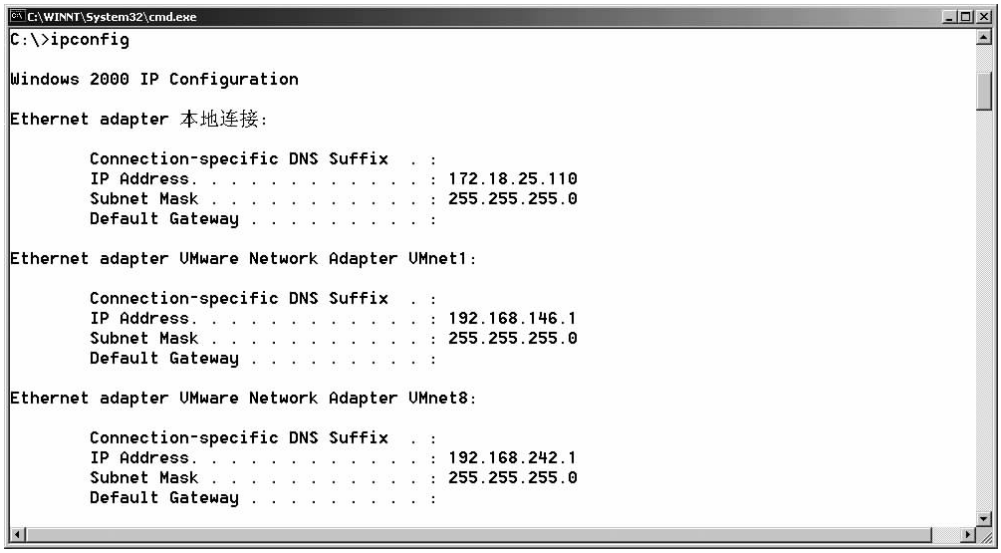

图 3-12　用 ipconfig 命令查看本机 IP 地址

IPv4 统计信息(IP、ICMP、TCP 和 UDP)。使用 netstat -an 命令可以查看目前活动的连接和开放的端口，是网络管理员查看网络是否被入侵的最简单方法，其方法如图 3-13 所示。如果状态为 LISTENING，表示端口正在被监听，还没有与其他主机相连；如果状态为 ESTABLISHED，表示正在与某主机连接并通信，同时显示该主机的 IP 地址和端口号。

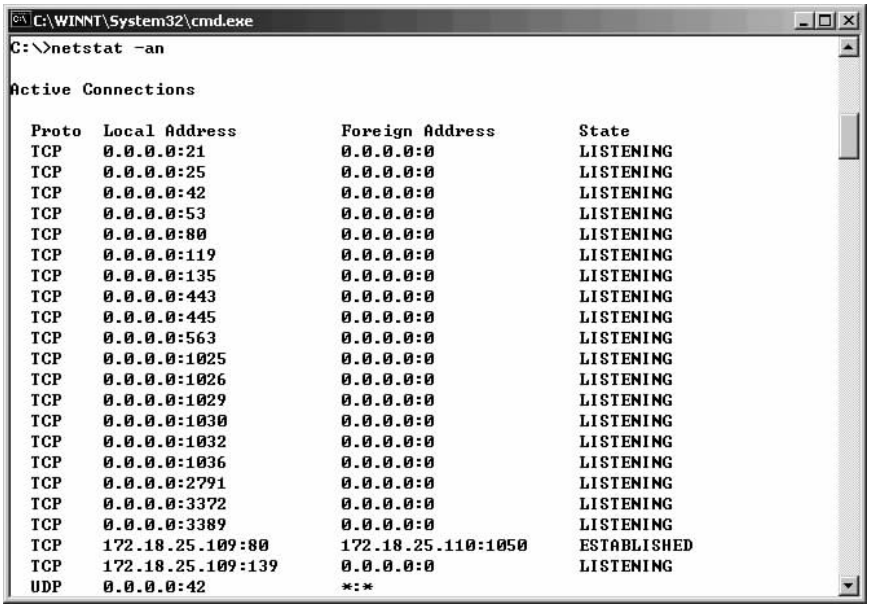

图 3-13　用 netstat -an 命令查看连接和开放端口

4. 查询、删除、修改用户信息应用

net 命令的主要功能是查看具体主机上的用户列表、添加和删除用户、与对方计算机建立连接、启动或者停止某网络服务等有关信息，便于进行管理。

【案例 3-7】 利用 net user 查看计算机上的用户列表，如图 3-14 所示。还可以用“net user＋用户名密码”为用户修改密码，如将管理员密码改为 123456，如图 3-15 所示。

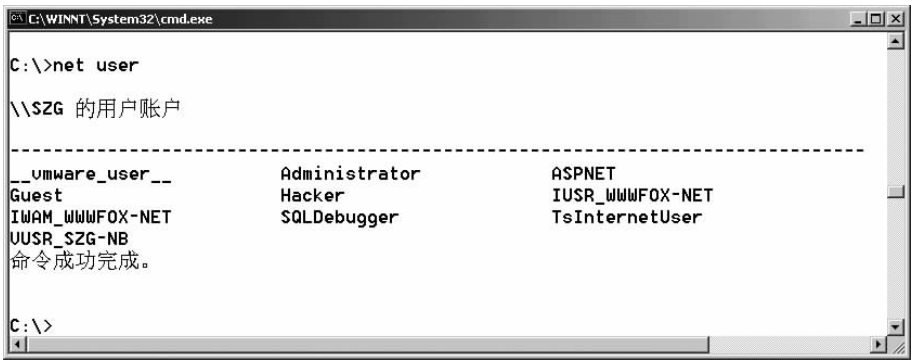

图 3-14 用 net user 查看计算机上的用户列表

图 3-15 用 net user 修改用户密码

【案例 3-8】 建立用户并添加到管理员组。

利用 net 命令可以新建一个用户名为 jack 的用户，然后，将此用户添加到密码为 123456 的管理员组，如图 3-16 所示。

案例名称：添加用户到管理员组

文件名称：3-1-1.bat

```
net user jack 123456 /add
net localgroup administrators jack /add
net user
```