“十二五”职业教育国家规划教材
经全国职业教育教材审定委员会审定

信息安全技术基础

主　编　鲁先志　武春岭
副主编　邹汪平　周璐璐

高等教育出版社

“十二五”职业教育国家规划教材
经全国职业教育教材审定委员会审定

信息安全技术基础

主　编　鲁先志　武春岭
副主编　邹汪平　周璐璐

XINXI ANQUAN JISHU JICHU

高等教育出版社·北京

内容提要

本书以 Windows 服务器版本操作系统为平台，通过介绍信息安全基本理论和常用安全技术，以任务驱动的方式引导学生完成项目实训，体现了任务驱动和“教学做”一体化的思想，实用性强。

本书的主要内容包括信息安全概述、操作系统活动目录安全管理、用户账户安全、操作系统访问控制、操作系统安全策略、操作系统恶意代码防范、操作系统备份与恢复、主机安全风险评估。各章都有针对相关信息安全理论知识的任务实训来帮助学生巩固该章所学知识。

本书内容丰富，文字浅显易懂，可作为高职高专信息安全、计算机应用和其他相关专业的教材，也可作为信息安全行业从业人员的自学参考书。

图书在版编目（CIP）数据

信息安全技术基础 / 鲁先志，武春岭主编. --北京：高等教育出版社，2016.11

ISBN 978-7-04-046363-7

Ⅰ. ① 信… Ⅱ. ① 鲁… ② 武… Ⅲ. ① 信息安全-安全技术-高等职业教育-教材 Ⅳ. ① TP309

中国版本图书馆 CIP 数据核字（2016）第 199481 号

策划编辑	郑期彤	责任编辑	郑期彤	封面设计	姜 磊	版式设计	于 婕
插图绘制	郝 林	责任校对	张小镝	责任印制	耿 轩		

出版发行	高等教育出版社	网 址	http://www.hep.edu.cn
社 址	北京市西城区德外大街 4 号		http://www.hep.com.cn
邮政编码	100120	网上订购	http://www.hepmall.com.cn
印 刷	中国农业出版社印刷厂		http://www.hepmall.com
开 本	787mm×1092mm 1/16		http://www.hepmall.cn
印 张	17.5		
字 数	370 千字	版 次	2016 年 11 月第 1 版
购书热线	010-58581118	印 次	2016 年 11 月第 1 次印刷
咨询电话	400-810-0598	定 价	29.80 元

物 料 号 46363-00

出 版 说 明

教材是教学过程的重要载体，加强教材建设是深化职业教育教学改革的有效途径，推进人才培养模式改革的重要条件，也是推动中高职协调发展的基础性工程，对促进现代职业教育体系建设，切实提高职业教育人才培养质量具有十分重要的作用。

为了认真贯彻《教育部关于“十二五”职业教育教材建设的若干意见》（教职成〔2012〕9号），2012年12月，教育部职业教育与成人教育司启动了“十二五”职业教育国家规划教材（高等职业教育部分）的选题立项工作。作为全国最大的职业教育教材出版基地，我社按照“统筹规划，优化结构，锤炼精品，鼓励创新”的原则，完成了立项选题的论证遴选与申报工作。在教育部职业教育与成人教育司随后组织的选题评审中，由我社申报的1338种选题被确定为“十二五”职业教育国家规划教材立项选题。现在，这批选题相继完成了编写工作，并由全国职业教育教材审定委员会审定通过后，陆续出版。

这批规划教材中，部分为修订版，其前身多为普通高等教育“十一五”国家级规划教材（高职高专）或普通高等教育“十五”国家级规划教材（高职高专），在高等职业教育教学改革进程中不断吐故纳新，在长期的教学实践中接受检验并修改完善，是“锤炼精品”的基础与传承创新的硕果；部分为新编教材，反映了近年来高职院校教学内容与课程体系改革的成果，并对接新的职业标准和新的产业需求，反映新知识、新技术、新工艺和新方法，具有鲜明的时代特色和职教特色。无论是修订版，还是新编版，我社都将发挥自身在数字化教学资源建设方面的优势，为规划教材开发配备数字化教学资源，实现教材的一体化服务。

这批规划教材立项之时，也是国家职业教育专业教学资源库建设项目及国家精品资源共享课建设项目深入开展之际，而专业、课程、教材之间的紧密联系，无疑为融通教改项目、整合优质资源、打造精品力作奠定了基础。我社作为国家专业教学资源库平台建设和资源运营机构及国家精品开放课程项目组织实施单位，将建设成果以系列教材的形式成功申报立项，并在审定通过后陆续推出。这两个系列的规划教材，具有作者队伍强大、教改基础深厚、示范效应显著、配套资源丰富、纸质教材与在线资源一体化设计的鲜明特点，将是职业教育信息化条件下，扩展教学手段和范围，推动教学方式方法变革的重要媒介与典型代表。

教学改革无止境，精品教材永追求。我社将在今后一到两年内，集中优势力量，全力以赴，出版好、推广好这批规划教材，力促优质教材进校园、精品资源进课堂，从而更好地服务于高等职业教育教学改革，更好地服务于现代职教体系建设，更好地服务于青年成才。

高等教育出版社

2014年7月

前　言

信息安全技术所涉及的知识面广且环境复杂，是困扰信息安全专业学生的一个主要问题。本书以主流操作系统 Windows Server 2003 为平台，结合相关基础知识，对信息安全技术作了系统全面的阐述。本书以企业实际工作中操作系统的安全部署和安全防范为切入点，将 Windows 系统安全与信息安全理论知识结合起来，通过将企业中的典型工作任务引入各个章节中，以利于学生接受的方式在书中表述，以利于“学”的方式对知识进行传递。

本书共包含 8 章 14 个任务，从信息安全概述开始展开，依次从操作系统活动目录安全管理、用户账户安全、操作系统访问控制、操作系统安全策略、操作系统恶意代码防范、操作系统备份与恢复、主机安全风险评估等方面，全面系统地介绍了信息安全中主机安全部分的基本理论和实际操作案例。

本书的最大特色是“易教易学”，主要体现在 3 个方面。

（1）内容实用，覆盖面广。本书的任务部分虽然以 Windows Server 2003 为平台，但所讲授的理论知识同样适用于 Linux 等相关操作系统。内容以国家对计算机信息系统的等级保护要求为主线，覆盖了整个主机测评的相关控制点，使学生学习后能够达到国家对信息系统安全从业人员专业知识的基本要求。

（2）理论与实践相结合。本书在讲授理论知识的基础上，提供了丰富的项目实践，把对学生应用能力的培养放在突出重要的位置，以增强学生的实际应用能力。

（3）由企业与院校联合开发。企业最了解哪些内容是经常用到的，需要学生了解和掌握，重点内容重点讲解；院校授课教师参与教材开发，可以使企业的经验以最利于学生接受的方式在书中表述，以最利于“学”的方式传递知识。

本书由重庆电子工程职业学院鲁先志、武春岭任主编，重庆电子工程职业学院周璐璐和池州职业技术学院邹汪平任副主编。具体分工如下：鲁先志负责组织策划并编写第 2 章、第 5 章和第 8 章，武春岭负责结构规划、统稿和最后修订并编写第 1 章，周璐璐编写第 6 章，邹汪平编写第 3 章、第 4 章和第 7 章。本书可提供 PPT 教学课件（标注图标为  ）、部分素材（标注图标为  ）及工具（标注图标为  ），读者可联系编辑获取（1548103297@qq.com）。此外，编者参阅了网络上关于同类内容的大量资料，在此对资料提供者表示感谢。

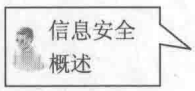
由于编者水平有限，书中疏漏之处在所难免，敬请专家与读者批评指正。编者邮箱为：lxz0665@sina.com。

编　者

2015 年 9 月

目　录

第1章
信息安全概述



知识目标

- 理解信息安全的概念。
- 理解网络安全防御体系的概念和作用。
- 理解安全域的概念。

技能目标

- 掌握 Windows Server 2003 操作系统的安装。
- 掌握 Windows Server 2003 操作系统的配置。

任务引导

信息作为一种资源，它的普遍性、共享性、增值性、可处理性和多效用性，使其对于人类具有特别重要的意义。信息安全的实质就是要保护信息系统或信息网络中的信息资源免受各种类型的威胁、干扰和破坏，即保证信息的安全。

Windows Server 2003 是中低端服务器中的主流操作系统，由美国微软公司开发。Windows 系列操作系统的最大优点就是其易用性，只要熟悉一般操作，就可以轻松构建和设置基本的网络服务。Windows Server 2003 操作系统的安装也比较简单，本章的任务实施部分将详细介绍 Windows Server 2003 操作系统的安装。

相关知识

1.1　信息安全基础

Windows Server 2003 操作系统是一套成熟的操作系统，拥有较高的使用率。所有系统管理员都已经认识到系统安全是网络管理工作中重要的，同时也是最基础的组成部分。

那么，如何做到操作系统的安全使用？操作系统的危险因素有哪些？首先要从信息安全的概念开始了解。

信息安全是指为数据处理系统而采取的技术的和管理的安全保护，保护计算机硬件、软件和数据不因偶然的或恶意的原因而遭到破坏、更改、泄露。这里面既包含了层面的概念，其中计算机硬件可以看作物理层面，软件可以看作运行层面，再就是数据层面；又包含了属性的概念，其中破坏涉及的是可用性，更改涉及的是完整性，泄露涉及的是保密性。

传统的信息安全概念，指网络与信息系统正常运行，防止网络与信息系统中的信息丢失、泄密以及未授权访问、修改或者删除。其核心是信息安全的 3 个基本属性，即保密性、完整性和可用性。

保密性：指信息不被泄露给非授权的用户、实体或进程，或被其利用

的特性。

完整性：指信息未经授权不能进行更改的特性，即信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、插入的特性。

可用性：指信息可被授权实体访问并按需求使用的特性。例如，在授权用户或实体需要信息服务时，信息服务应该可以使用，或者是信息系统部分受损或需要降级使用时，能为授权用户提供有效服务。

随着信息化的发展，信息安全的内涵不断深化，外延不断拓展。当前，国民经济和社会发展对信息化高度依赖，信息安全已经发展成为涉及国民经济和社会发展各个领域，不仅影响公民个人权益，更关乎国家安全、经济发展、公众利益的重大战略问题。党的十六届四中全会将信息安全作为国家安全的重要组成部分，明确提出要“增强国家安全意识，完善国家安全战略”，并确保“国家的政治安全、经济安全、文化安全和信息安全”。

简而言之，新形势下的信息安全，就是要保障信息化健康发展，防止信息化发展过程中出现的各种消极和不利因素。这些消极和不利因素不但根源于信息可能被非授权窃取、修改、删除以及信息系统可能被非授权中断，也因违法与不良信息的传播与扩散而表现为信息内容安全问题。其影响不再局限于信息与信息系统自身，还外延至国家的政治、经济、文化、军事等各个方面。

1.2 网络安全防御体系

随着计算机技术和 Internet 的发展，各种利用系统安全弱点的新型攻击大量地被入侵者所使用，网络攻击群体出于各种目的，在规模上正迅速扩大，技能水平飞速增强，攻击所造成的影响日益严重，信息系统所面临的安全风险和威胁日趋严重，网络信息安全已成为当今互联网发展需要做好的最重要的工作。

全方位的、整体的网络安全防范体系也是分层次的，不同层次反映了不同的安全问题，根据网络的应用现状情况和网络的结构，安全防范体系的层次可划分为物理层安全、系统层安全、网络层安全、应用层安全和管理层安全。

（1）物理层安全

该层次的安全包括通信线路的安全、物理设备的安全、机房的安全等。物理层安全主要体现在通信线路的可靠性（线路备份、网管软件、传输介质），软硬件设备安全性（替换设备、拆卸设备、增加设备），设备的备份，防灾害能力、防干扰能力，设备的运行环境（温度、湿度、烟尘），不间断电源保障等方面。

（2）系统层安全

该层次的安全问题来自网络内使用的操作系统的安全，如 Windows NT、Windows 2000 等。主要表现在三方面：一是操作系统本身的缺陷带来的不安全因素，主要包括身份认证、访问控制、系统漏洞等；二是对操

作系统的安全配置问题；三是病毒对操作系统的威胁。

（3）网络层安全

该层次的安全问题主要体现在网络方面的安全性，包括网络层身份认证、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、入侵检测的手段、网络设施防病毒等。

（4）应用层安全

该层次的安全问题主要由提供服务所采用的应用软件和数据的安全性产生，包括 Web 服务、电子邮件系统、DNS 等。此外，还包括病毒对系统的威胁。

（5）管理层安全

安全管理包括安全技术和设备的管理、安全管理制度、部门与人员的组织规则等。管理的制度化在很大程度上影响着整个网络的安全，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 安全域的概念

随着经济的快速发展，业务需求成倍增加，计算机系统的功能不断增强，其网络复杂程度也在不断提高；各单位内部系统与外部各系统信息交换的需求也不断增长，主要包括外部信息的流入和内部信息的流出。系统的核心数据信息，一方面面临数据受灾、泄露等影响较大的威胁，另一方面面临蠕虫等扩散导致网络拥塞、系统误操作导致数据破坏或应用中断等可能性较高的威胁。核心数据信息的安全防护重点在于信息的可用性、机密性、完整性和不可抵赖性。分析目前网络的现状，主要存在以下安全问题。

① 网络边界不够清晰，对网络内各部分的安全需求缺乏统一规划，没有对核心业务系统的访问进行很好的控制，各接入系统之间没有进行明确的访问控制，网络之间彼此可以互相访问，系统局部的安全问题极易扩散到整个系统。

② 计算机系统急速膨胀，网络结构快速变化，原有网络安全结构明显滞后，网络安全威胁级别增高，漏洞范围增加，安全风险加大，甚至超出可忍受的水平。

为此，只有从纵深的角度，全盘考虑安全的部署和拓展应用，才能应对日趋复杂的网络环境。面对多样复杂的安全威胁需求，原有的局部网络安全防护难以适应目前的需要，建立纵深防御体系，防止因局部的侵入导致整个系统的崩溃成为必然选择。纵深防御思想从多个层面，根据系统中各部分的数据信息重要程度、资产等级的不同对安全需求也不同的特点，按照分治法的思想将系统中有相同安全需求的部分划分成不同的安全域来保障信息与信息系统的安全。安全域是一个紧密联系的整体，相互间既有纵向的纵深关系，

又有横向的协作关系，每个范围都有各自的安全目标和安全保障职责，通过积极防御、综合防范的方针为各个保护范围提供安全保障，有效协调纵向和横向关系，提高网络整体防御能力。

网络安全域是指同一系统内有相同的安全保护需求，相互信任，并具有相同的安全访问控制和边界控制策略的子网或网络，且相同的网络安全域共享一样的安全策略。广义的安全域可理解为具有相同业务要求和安全要求的 IT 系统要素的集合。网络安全域从大的方面一般可划分为本地网络、远程网络、公共网络和伙伴访问 4 个部分。在不同的安全域之间需要设置防火墙以进行安全保护。

1.4 Windows Server 2003 的安全性能

企业已经通过 Intranet、Extranet 和 Internet 站点的合成扩展了传统意义上的局域网（LAN）的含义。因此，扩大了的系统的安全问题比从前更为重要。为了提供一个安全环境，Windows Server 2003 操作系统可提供很多重要的新安全特性，以及一些在 Windows 2000 Server 原有安全特性基础上的改进。

1. 新安全特性

（1）高信度计算

病毒的存在及软件安全性是现存的一个持续性的挑战。为了解决该问题，微软公司在其所有产品上使用了高可信度计算作为关键技术。高可信度计算为设备的开发提供了一个框架，这些由计算机及软件给予动力的设备就如同每天在家使用的家用电器和日用品一样安全可靠。尽管现在真正的高可信度计算平台还未出现，经过了重新设计的 Windows Server 2003 正朝向这一目标踏出了坚实的一步。

（2）通用语言运行时

通用语言运行时（Common Language Runtime）软件引擎是 Windows Server 2003 提升可靠性并确保安全计算环境的关键要素。它降低了由通常编程错误引起的 bug 和安全漏洞的数量，因而也减少了可供攻击者利用的漏洞。

通用语言运行时检验应用程序是否能够正常运行，并检查是否具备适当的安全许可，确保代码仅完成适当的操作。它通过检查代码下载和安装的位置、是否拥有可信的开发商的数字签名以及签名后代码是否曾被改动，来完成上述任务。

2. 优势

Windows Server 2003 可为商务活动提供更安全、更经济的平台，其优势见表 1-1。