

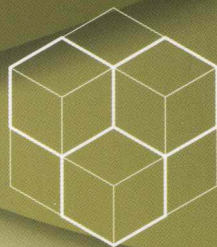


全国高校应用人才培养规划教材·网络技术系列

WANGLUO ANQUAN GUANLI JISHU XIANGMUHUA JIAOCHENG

网络安全管理技术项目化教程

丁喜纲 主编



Network
Tech



北京大学出版社
PEKING UNIVERSITY PRESS

普通高等教育“十二五”规划教材

全国高校应用人才培养规划教材·网络技术系列

网络安全管理技术项目化教程

主 编 丁喜纲



北京大学出版社
PEKING UNIVERSITY PRESS

内 容 简 介

本书以中小型企业网络安全管理为主要工作情境,采用项目/任务模式,将计算机网络安全管理相关知识综合到各项技能中。本书包括 10 个工作项目,分别是认识网络安全管理、Windows 桌面系统安全管理、Windows 服务器系统安全管理、网络物理基础设施安全管理、网络设备安全管理、安装与部署网络安全设备、保障数据传输安全、实现网络冗余和数据备份、无线局域网安全管理和使用网络安全管理工具。

本书主要面向网络安全管理技术的初学者,读者可以在阅读本书时同步进行实训,从而掌握网络安全管理方面的基础知识和实践技能。本书可以作为大中专院校相关课程的教材,也适合从事网络管理、维护等工作的技术人员以及网络技术爱好者参考使用。

图书在版编目(CIP)数据

网络安全管理技术项目化教程/丁喜纲主编. —北京:北京大学出版社,2012.11

(全国高校应用人才培养规划教材·网络技术系列)

ISBN 978-7-301-21479-4

I. ①网… II. ①丁… 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(2012)第 254861 号

书 名: 网络安全管理技术项目化教程

著作责任者: 丁喜纲 主编

策 划 编 辑: 吴坤娟

责 任 编 辑: 桂 春

标 准 书 号: ISBN 978-7-301-21479-4/TP·1256

出 版 发 行: 北京大学出版社

地 址: 北京市海淀区成府路 205 号 100871

网 址: <http://www.pup.cn> 电子信箱: zyjy@pup.cn

电 话: 邮购部 62752015 发行部 62750672 编辑部 62765126 出版部 62754962

印 刷 者: 三河市博文印刷厂

经 销 者: 新华书店

787 毫米×1092 毫米 16 开本 23.25 印张 580 千字

2012 年 11 月第 1 版 2012 年 11 月第 1 次印刷

定 价: 44.00 元

未经许可,不得以任何方式复制或抄袭本书之部分或全部内容。

版权所有,侵权必究

举报电话: (010)62752024 电子信箱: fd@pup.pku.edu.cn

前 言

随着计算机网络应用的不断普及,网络资源和网络应用服务日益丰富,计算机网络安全问题已经成为网络建设和发展中的热门话题。在网络管理过程中,必须采取相应措施,保证网络系统连续、可靠、正常地运行,网络服务不中断;并且应保护系统中的硬件、软件及数据,使其不因偶然的或者恶意的原因而遭到破坏、更改和泄露。因此,作为网络技术相关专业的学生和技术人员,必须掌握网络安全管理的知识,并具备真正的技术应用能力。

本书在编写时贯穿了“以职业活动为导向,以职业技能为核心”的理念,结合工程实际,反映岗位需求,以中小型企业网络安全管理为主要工作情境,采用项目/任务模式,将计算机网络安全管理相关知识综合到各项技能中。本书包括10个工作项目,分别是认识网络安全管理、Windows桌面系统安全管理、Windows服务器系统安全管理、网络物理基础设施安全管理、网络设备安全管理、安装与部署网络安全设备、保障数据传输安全、实现网络冗余和数据备份、无线局域网安全管理和使用网络安全管理工具。每个项目由需要读者亲自动手完成的工作任务组成,读者可以在阅读本书时同步进行实训,从而掌握网络安全管理方面的基础知识和实践技能。

本书主要特点如下。

(1) 以工作过程为导向,采用项目/任务模式。本书以中小型企业网络安全管理为主要工作情境,采用项目/任务模式,力求使读者在做中学、在学中做,真正能够利用所学知识解决实际问题,形成职业能力。

(2) 紧密结合教学实际。目前,市面上计算机网络的相关产品种类很多,管理与配置方法各不相同。考虑到读者的实际实验条件,本书主要选择了具有代表性并且被广泛使用的Microsoft和Cisco公司的产品为例,读者可以利用VMware、Cisco Packet Tracer等软件在一台计算机上完成本书的绝大部分工作任务。另外,本书每个项目后都附有习题,分为思考问答和技能操作,有利于读者思考并检查学习效果。

(3) 参照职业标准。职业标准源自生产一线,源自工作过程,因此本书在编写时参照了《计算机网络管理员国家职业标准》及其他相关职业标准和企业认证中的要求,突出了职业特色和岗位特色。

(4) 开放式的结构。网络安全管理涉及网络的各个方面,不同的网络环境采用的安全管理技术也不相同。本书在每个工作任务中增加了“技能拓展”模块,引导读者在掌握基本知识和技能的前提下,自主地了解与本次任务相关的其他技术和产品,培养自我学习能力,以适用职业发展的需要。

本书主要面向网络安全管理技术的初学者,可以作为大中专院校相关课程的教材,也适合从事网络管理、维护等工作的技术人员以及网络技术爱好者参考使用。

本书由丁喜纲主编,边金良、安述照参与了部分内容的编写工作。本书在编写过程中参考了国内外网络安全管理方面的著作和文献,并查阅了Internet上公布的很多相关资料,



由于 Internet 上的资料引用复杂，所以很难注明原出处，在此对所有作者致以衷心的感谢。

编者意在为读者奉献一本实用并具有特色的教材，但由于网络安全管理涉及的内容很多，技术发展日新月异，加之我们水平有限，书中难免有错误和不妥之处，敬请广大读者批评指正。

编 者

2012 年 9 月

目 录

项目 1 认识网络安全管理	(1)
任务1.1 认识网络的脆弱性	(1)
【任务目的】	(1)
【工作环境与条件】	(1)
【相关知识】	(1)
1.1.1 网络安全的基本要素	(1)
1.1.2 网络面临的安全威胁	(2)
【任务实施】	(4)
操作 1 分析某企业网络的安全隐患	(4)
操作 2 分析校园网的安全风险	(5)
【技能拓展】	(5)
任务1.2 体验网络攻击	(6)
【任务目的】	(6)
【工作环境与条件】	(6)
【相关知识】	(6)
1.2.1 网络攻击概述	(6)
1.2.2 常见网络攻击手段	(6)
【任务实施】	(10)
操作 1 利用 X-Scan 侦测目标主机	(10)
操作 2 利用 SMB Cracker 破解主机账户密码	(12)
操作 3 利用 IPC \$ 入侵远程主机	(14)
操作 4 体验木马攻击	(16)
【技能拓展】	(19)
任务1.3 规划网络整体安全	(20)
【任务目的】	(20)
【工作环境与条件】	(20)
【相关知识】	(20)
1.3.1 网络安全策略	(20)
1.3.2 常用网络安全措施	(21)
1.3.3 典型网络安全问题的解决方案	(23)
【任务实施】	(24)
操作 1 分析校园网工程案例	(24)
操作 2 分析企业网工程案例	(24)
【技能拓展】	(24)
习题 1	(25)
1. 思考与问答	(25)



2. 技能操作	(26)
项目2 Windows 桌面系统安全管理	(27)
任务2.1 设置系统安全访问权限	(27)
【任务目的】	(27)
【工作环境与条件】	(27)
【相关知识】	(27)
2.1.1 Windows 系统的安全访问组件	(27)
2.1.2 Windows 系统的用户权利	(28)
2.1.3 Windows 系统的用户权限	(29)
2.1.4 Windows 系统的共享权限	(31)
【任务实施】	(32)
操作1 用户账户安全设置	(32)
操作2 设置 NTFS 权限	(36)
操作3 设置共享权限	(38)
【技能拓展】	(39)
任务2.2 使用文件加密系统	(40)
【任务目的】	(40)
【工作环境与条件】	(40)
【相关知识】	(40)
2.2.1 加密与解密	(40)
2.2.2 加密文件系统 (EFS)	(40)
【任务实施】	(41)
操作1 利用 EFS 进行文件加密	(41)
操作2 授权其他用户访问加密文件	(42)
【技能拓展】	(45)
任务2.3 维护注册表安全	(45)
【任务目的】	(45)
【工作环境与条件】	(45)
【相关知识】	(45)
2.3.1 注册表的结构	(45)
2.3.2 注册表的配置单元	(46)
【任务实施】	(47)
操作1 设置注册表用户访问权限	(47)
操作2 导出和导入注册表	(47)
操作3 利用注册表进行系统安全设置	(48)
【技能拓展】	(49)
任务2.4 使用本地安全策略和组策略	(49)
【任务目的】	(49)
【工作环境与条件】	(50)
【相关知识】	(50)



【任务实施】	(50)
操作1 设置本地安全策略	(50)
操作2 设置组策略	(55)
【技能拓展】	(57)
任务2.5 系统漏洞检测与补丁安装	(57)
【任务目的】	(57)
【工作环境与条件】	(57)
【相关知识】	(58)
2.5.1 系统漏洞	(58)
2.5.2 补丁程序	(59)
【任务实施】	(59)
操作1 系统漏洞检测	(59)
操作2 关闭不必要的服务和端口	(61)
操作3 设置系统自动更新	(64)
【技能拓展】	(64)
任务2.6 设置系统防火墙	(65)
【任务目的】	(65)
【工作环境与条件】	(65)
【相关知识】	(65)
2.6.1 防火墙的功能	(65)
2.6.2 防火墙的实现技术	(66)
2.6.3 Windows 系统防火墙	(67)
【任务实施】	(67)
操作1 启用系统防火墙	(67)
操作2 设置系统防火墙允许 ping 命令运行	(69)
操作3 设置系统防火墙允许应用程序运行	(69)
【技能拓展】	(69)
任务2.7 使用安全审计和性能监控	(69)
【任务目的】	(69)
【工作环境与条件】	(70)
【相关知识】	(70)
2.7.1 Windows 系统的审核	(70)
2.7.2 Windows 事件日志文件	(71)
【任务实施】	(71)
操作1 设置审核策略	(71)
操作2 设置审核对象	(72)
操作3 使用事件查看器	(72)
操作4 使用任务管理器	(74)
操作5 使用性能监视器	(75)
【技能拓展】	(78)



习题 2	(79)
1. 思考与问答	(79)
2. 技能操作	(79)
项目 3 Windows 服务器系统安全管理	(82)
任务3.1 Active Directory 服务安全管理	(82)
【任务目的】	(82)
【工作环境与条件】	(82)
【相关知识】	(82)
3.1.1 Active Directory 的基本概念	(82)
3.1.2 域用户账户和组账户	(83)
3.1.3 域信任关系	(86)
【任务实施】	(87)
操作 1 用户与计算机基本安全设置	(87)
操作 2 利用组策略进行安全管理	(90)
操作 3 建立和管理域信任关系	(92)
操作 4 组织单位的委派控制	(96)
【技能拓展】	(96)
任务3.2 DHCP 服务安全管理	(96)
【任务目的】	(96)
【工作环境与条件】	(97)
【相关知识】	(97)
3.2.1 DHCP 的运行过程	(97)
3.2.2 DHCP 服务器的授权	(98)
【任务实施】	(99)
操作 1 DHCP 服务器的授权与审核	(99)
操作 2 为客户机保留特定的 IP 地址	(99)
操作 3 配置 DHCP 选项	(100)
操作 4 安装多台 DHCP 服务器	(100)
操作 5 配置 DHCP 中继代理	(101)
操作 6 维护 DHCP 数据库	(104)
【技能拓展】	(105)
任务3.3 DNS 服务安全管理	(105)
【任务目的】	(105)
【工作环境与条件】	(105)
【相关知识】	(106)
3.3.1 DNS 服务器的类型	(106)
3.3.2 DNS 区域的类型	(106)
3.3.3 DNS 服务的查找模式	(107)



【任务实施】	(108)
操作1 管理 Hosts 文件	(108)
操作2 建立辅助区域和存根区域	(108)
操作3 DNS 区域安全管理	(110)
操作4 求助于其他 DNS 服务器	(113)
【技能拓展】	(114)
任务3.4 Internet 信息服务 (IIS) 安全管理	(114)
【任务目的】	(114)
【工作环境与条件】	(114)
【相关知识】	(114)
【任务实施】	(115)
操作1 网站安全管理	(115)
操作2 FTP 站点安全管理	(119)
操作3 利用 HTML 远程管理 IIS	(121)
【技能拓展】	(122)
习题3	(123)
1. 思考与问答	(123)
2. 技能操作	(123)
项目4 网络物理基础设施安全管理	(126)
任务4.1 网络布线系统安全管理	(126)
【任务目的】	(126)
【工作环境与条件】	(126)
【相关知识】	(126)
4.1.1 网络布线系统的结构和组成	(126)
4.1.2 网络配线设备	(128)
4.1.3 网络布线系统的管理	(129)
4.1.4 网络布线系统的安全要求	(131)
【任务实施】	(134)
操作1 走访校园网综合布线工程	(134)
操作2 走访企业网综合布线工程	(134)
【技能拓展】	(134)
任务4.2 网络机房环境安全管理	(134)
【任务目的】	(134)
【工作环境与条件】	(135)
【相关知识】	(135)
4.2.1 网络机房场地环境安全	(135)
4.2.2 网络机房运行环境安全	(137)
【任务实施】	(137)
操作1 参观网络机房	(137)



操作 2 认识和操作机房空调系统	(138)
操作 3 认识和操作机房消防系统	(138)
【技能拓展】	(139)
任务4.3 保障网络设备的物理安全	(140)
【任务目的】	(140)
【工作环境与条件】	(140)
【相关知识】	(140)
4.3.1 网络设备物理安全的一般要求	(140)
4.3.2 网络设备的供配电	(141)
4.3.3 UPS	(142)
【任务实施】	(144)
操作 1 认识网络的供配电系统	(144)
操作 2 使用和维护 UPS	(144)
【技能拓展】	(146)
习题 4	(147)
1. 思考与问答	(147)
2. 技能操作	(147)
项目 5 网络设备安全管理	(148)
任务5.1 配置 ACL	(148)
【任务目的】	(148)
【工作环境与条件】	(148)
【相关知识】	(148)
5.1.1 ACL 概述	(148)
5.1.2 ACL 的执行过程	(149)
5.1.3 ACL 的类型	(149)
【任务实施】	(150)
操作 1 配置标准 ACL	(150)
操作 2 配置扩展 ACL	(152)
操作 3 配置命名 ACL	(154)
【技能拓展】	(155)
任务5.2 保障网络设备管理访问安全	(155)
【任务目的】	(155)
【工作环境与条件】	(155)
【相关知识】	(155)
5.2.1 网络设备的管理访问方式	(155)
5.2.2 用户账户和特权级别	(157)
5.2.3 AAA 安全服务体系	(157)
【任务实施】	(160)
操作 1 网络设备安全访问的基本设置	(160)



操作 2 设置用户账户和特权	(162)
操作 3 配置 AAA	(163)
操作 4 禁用不必要的功能和协议	(165)
【技能拓展】	(167)
任务5.3 路由协议安全管理	(167)
【任务目的】	(167)
【工作环境与条件】	(167)
【相关知识】	(167)
5.3.1 路由控制与过滤	(168)
5.3.2 路由协议的认证	(168)
【任务实施】	(169)
操作 1 RIP 安全设置	(169)
操作 2 OSPF 安全设置	(170)
【技能拓展】	(172)
任务5.4 网络接入层安全管理	(172)
【任务目的】	(172)
【工作环境与条件】	(172)
【相关知识】	(172)
5.4.1 端口安全和端口阻塞	(173)
5.4.2 风暴控制和端口隔离	(173)
5.4.3 PVLAN	(174)
5.4.4 交换机访问控制列表	(174)
5.4.5 动态 ARP 监控 (DAI)	(175)
【任务实施】	(176)
操作 1 配置端口安全	(176)
操作 2 配置 PVLAN	(177)
操作 3 配置交换机访问列表	(178)
操作 4 配置 DAI	(180)
【技能拓展】	(181)
习题 5	(181)
1. 思考与问答	(181)
2. 技能操作	(181)
项目 6 安装与部署网络安全设备	(184)
任务6.1 安装与部署防病毒系统	(184)
【任务目的】	(184)
【工作环境与条件】	(184)
【相关知识】	(184)
6.1.1 计算机病毒及其防御	(184)
6.1.2 局域网防病毒方案	(185)



6.1.3 企业级防病毒系统的选择	(186)
【任务实施】	(187)
操作1 认识 Symantec Endpoint Protection	(187)
操作2 安装与配置 Symantec Endpoint Protection Manager	(188)
操作3 配置和部署客户端软件	(190)
操作4 管理 Symantec Endpoint Protection	(193)
【技能拓展】	(195)
任务6.2 安装与部署企业级防火墙	(195)
【任务目的】	(195)
【工作环境与条件】	(196)
【相关知识】	(196)
6.2.1 ISA Server 的多网络结构	(196)
6.2.2 ISA Server 的网络规则	(198)
6.2.3 ISA Server 的防火墙策略	(198)
【任务实施】	(200)
操作1 安装 ISA Server	(200)
操作2 新建访问规则	(201)
操作3 配置 ISA 客户端接入 Internet	(203)
操作4 发布内部网络服务	(205)
【技能拓展】	(209)
任务6.3 安装与部署入侵检测系统	(209)
【任务目的】	(209)
【工作环境与条件】	(209)
【相关知识】	(209)
6.3.1 入侵检测系统的作用	(210)
6.3.2 入侵检测系统的分类	(210)
6.3.3 入侵检测系统的工作流程	(211)
6.3.4 入侵检测系统的部署方式	(212)
【任务实施】	(212)
操作1 认识与部署 Snort	(212)
操作2 安装 Snort	(214)
操作3 配置和运行 Snort	(217)
【技能拓展】	(219)
习题6	(219)
1. 思考与问答	(219)
2. 技能操作	(219)
项目7 保障数据传输安全	(221)
任务7.1 使用 PGP 加密工具	(221)
【任务目的】	(221)
【工作环境与条件】	(221)



【相关知识】	(221)
7.1.1 公开密钥加密	(221)
7.1.2 数字签名	(222)
7.1.3 PGP 加密工具	(223)
【任务实施】	(224)
操作1 安装 PGP	(224)
操作2 创建和保存密钥对	(224)
操作3 加密、解密文件	(225)
操作4 数字签名及验证	(226)
操作5 加密、解密邮件	(227)
【技能拓展】	(229)
任务7.2 安装 CA 与应用数字证书	(229)
【任务目的】	(229)
【工作环境与条件】	(229)
【相关知识】	(229)
7.2.1 PKI 概述	(229)
7.2.2 数字证书	(230)
7.2.3 证书认证机构 (CA)	(230)
【任务实施】	(231)
操作1 安装证书服务并架设独立根 CA	(231)
操作2 申请和颁发数字证书	(233)
操作3 利用数字证书实现邮件加密和数字签名	(236)
操作4 利用数字证书对文档签名	(238)
【技能拓展】	(239)
任务7.3 利用 SSL 实现网站安全连接	(239)
【任务目的】	(239)
【工作环境与条件】	(239)
【相关知识】	(240)
7.3.1 SSL 的作用	(240)
7.3.2 SSL 的工作过程	(240)
【任务实施】	(240)
操作1 在网站上建立证书申请文件	(240)
操作2 申请证书并下载证书文件	(242)
操作3 安装证书并启用 SSL	(243)
操作4 保存网站的证书	(245)
【技能拓展】	(246)
任务7.4 设置与应用 IPSec	(246)
【任务目的】	(246)
【工作环境与条件】	(246)



【相关知识】	(246)
7.4.1 IPsec 概述	(246)
7.4.2 IKE 协议	(247)
7.4.3 IPsec 的通信模式	(247)
【任务实施】	(248)
操作1 启用 IPsec	(248)
操作2 设置 IPsec 策略	(249)
【技能拓展】	(251)
任务7.5 配置 VPN 连接	(251)
【任务目的】	(251)
【工作环境与条件】	(252)
【相关知识】	(252)
7.5.1 VPN 概述	(252)
7.5.2 VPN 的相关技术和协议	(253)
【任务实施】	(254)
操作1 配置 PPTP VPN	(254)
操作2 配置 L2TP/IPsec VPN	(258)
【技能拓展】	(260)
习题7	(260)
1. 思考与问答	(260)
2. 技能操作	(260)
项目8 实现网络冗余和数据备份	(262)
任务8.1 实现网络设备冗余连接	(262)
【任务目的】	(262)
【工作环境与条件】	(262)
【相关知识】	(262)
8.1.1 网络设备的冗余部署	(262)
8.1.2 链路级冗余技术	(263)
8.1.3 网关级冗余技术	(265)
【任务实施】	(266)
操作1 配置端口聚合	(266)
操作2 配置生成树协议	(267)
操作3 配置 HSRP	(269)
操作4 配置双核心网络	(270)
【技能拓展】	(275)
任务8.2 利用 RAID 实现系统容错	(275)
【任务目的】	(275)
【工作环境与条件】	(275)
【相关知识】	(275)
8.1.1 服务器系统冗余技术	(275)



8.1.2 RAID	(276)
8.1.3 基本磁盘和动态磁盘	(276)
【任务实施】	(278)
操作1 获得动态磁盘	(278)
操作2 创建动态卷	(279)
操作3 动态磁盘的数据恢复	(280)
【技能拓展】	(282)
任务8.3 Windows 系统下的数据备份与恢复	(282)
【任务目的】	(282)
【工作环境与条件】	(282)
【相关知识】	(282)
8.3.1 数据备份概述	(282)
8.3.2 Windows 系统的备份标记	(284)
8.3.3 Windows 系统的备份类型	(284)
8.3.4 Windows 系统的备份方案	(285)
【任务实施】	(286)
操作1 查看备份标记	(286)
操作2 备份文件或文件夹	(286)
操作3 备份系统状态数据	(287)
操作4 还原文件和文件夹	(287)
操作5 使用备份计划自动完成备份	(288)
【技能拓展】	(291)
任务8.4 网络设备的数据备份与恢复	(292)
【任务目的】	(292)
【工作环境与条件】	(292)
【相关知识】	(292)
8.4.1 简单文件传输协议 (Trivial File Transfer Protocol, TFTP)	(292)
8.4.2 Cisco IOS 文件系统	(292)
【任务实施】	(293)
操作1 构建 TFTP 服务器	(293)
操作2 备份与恢复 Cisco IOS	(294)
操作3 备份与恢复 Cisco 配置文件	(296)
【技能拓展】	(297)
习题8	(297)
1. 思考与问答	(297)
2. 技能操作	(297)
项目9 无线局域网安全管理	(300)
任务9.1 WLAN 安全基本设置	(300)
【任务目的】	(300)



【工作环境与条件】	(300)
【相关知识】	(300)
9.1.1 无线局域网概述	(300)
9.1.2 无线局域网的安全问题	(302)
9.1.3 无线局域网的安全措施	(303)
【任务实施】	(305)
操作1 无线路由器基本安全设置	(305)
操作2 无线客户端基本安全设置	(308)
【技能拓展】	(310)
任务9.2 配置 IEEE 802.1x 用户身份认证	(310)
【任务目的】	(310)
【工作环境与条件】	(310)
【相关知识】	(311)
9.2.1 IEEE 802.1x	(311)
9.2.2 EAP	(312)
9.2.3 Internet 验证服务 (Internet Authentication Service, IAS)	(313)
【任务实施】	(313)
操作1 安装并设置 IAS 服务器	(313)
操作2 设置接入控制单元	(318)
操作3 设置无线客户端	(318)
【技能拓展】	(320)
任务9.3 无线局域网的 VLAN 部署	(320)
【任务目的】	(320)
【工作环境与条件】	(320)
【相关知识】	(320)
9.3.1 无线局域网中的 VLAN	(320)
9.3.2 无线局域网中的广播域	(321)
【任务实施】	(321)
【技能拓展】	(324)
习题9	(324)
1. 思考与问答	(324)
2. 技能操作	(324)
项目10 使用网络安全管理工具	(326)
任务10.1 构建 SNMP 网络管理环境	(326)
【任务目的】	(326)
【工作环境与条件】	(326)