



灵创职业教育·网络与信息安全系列教材

信息安全产品与方案

李 剑 等编著



北京邮电大学出版社
www.buptpress.com

Leader
灵创

灵创职业教育·网络与信息安全系列教材

信息安全标准与法规

网络攻击与防护技术

网络与信息安全综合实践教程

计算机病毒防护

信息安全产品与方案

信息安全管理与工程



XINXI ANQUAN CHANPIN YU FANGAN

策划人: 周 明
责任编辑: 崔 珞
封面设计: 七星工作室

ISBN 978-7-5635-1680-3



9 787563 516803 >

定价: 24.00 元



本书电子教案下载请登录
<http://buptpress.com/xzzx.asp>

灵创职业教育·网络与信息安全系列教材

信息安全产品与方案

李 剑 等编著

北京邮电大学出版社

·北京·

内 容 简 介

作为一本信息安全教材,本书介绍了信息安全领域常用的产品与方案。书中内容共12章。第1章是信息安全与信息安全产品。第2章是防火墙产品与方案。第3章是入侵检测产品与方案。第4章是虚拟专用网络产品与方案。第5章是网络隔离与网闸产品与方案。第6章是数据备份产品与方案。第7章是防病毒产品与方案。第8章是审计系统产品与方案。第9章是安全扫描器产品与方案。第10章是反恶意软件产品与方案。第11章是其他信息安全产品与方案。第12章是信息安全整体解决方案。除了以上内容之外,书中还介绍了大量的实验和实践内容。

本书适合于高等职业技术学校或大学专科信息安全相关专业的学生进行信息安全产品与方案方面的教育。

图书在版编目(CIP)数据

信息安全产品与方案/李剑等编著. —北京:北京邮电大学出版社,2008.6

ISBN 978-7-5635-1680-3

I. 信… II. 李… III. 信息系统—安全技术—教材 IV. TP309

中国版本图书馆 CIP 数据核字(2008)第 050265 号

书 名: 信息安全产品与方案

作 者: 李剑 等

责任编辑: 崔 璐

出版发行: 北京邮电大学出版社

社 址: 北京市海淀区西土城路 10 号(邮编:100876)

发 行 部: 电话: 010-62282185 传真: 010-62283578

E-mail: publish@bupt.edu.cn

经 销: 各地新华书店

印 刷: 北京市梦宇印务有限公司

开 本: 787 mm×1 092 mm 1/16

印 张: 13.75

字 数: 341 千字

印 数: 1—5 000 册

版 次: 2008 年 6 月第 1 版 2008 年 6 月第 1 次印刷

ISBN 978-7-5635-1680-3

定 价: 24.00 元

• 如有印装质量问题,请与北京邮电大学出版社发行部联系 •

灵创职业教育·网络与信息安全系列教材

编 委 会

名誉主任 方滨兴 院士

主 任 杨义先

委 员 (排名不分先后)

周继军 陈 运 方 勇 韩 臻

李子臣 罗 平 姬东耀 陈绥阳

姚景平 刘吉强 马兆丰 范科锋

辛 阳 郑康锋 李祥学 王励成

李宝安 赵金满 刘海云 李同芳

田 华 李 剑

序

目前我国“职业教育”正值春天。在党和国家的大力支持和积极推动下,全社会对职业教育的关注空前高涨,职业教育蓬勃发展。值此大好时机,每个教育工作者都应认真贯彻落实科学的发展观,坚持以服务为宗旨,以就业为导向,以提高质量为重点,进一步解放思想、开拓进取、扎实有力地推进我国职业教育又好又快地发展,办好人民满意的职业教育。但出于历史原因,目前我国职业教育体系很不健全,职教专业、职教教材“本科简化型”现象比较普遍,真正“重实践,重应用,与职业技能培养紧密结合”的高质量精品教材非常紧缺。

鉴于上述情况,为促进我国职业教育的规范发展,特别是为了满足当前各级各类职业教育教师、学生对适配自身教育和实践教材的迫切需要,北京邮电大学出版社,灵创团队北京邮电大学信息安全中心,灵创团队北京邮电大学数字内容研究中心以及绵阳灵创电子信息技术的专家、领导,决定共同合作,团结全国相关领域专家,策划、撰写、出版多套覆盖“网络与信息安全”和“数字媒体创意”等领域的“灵创职业教育”系列教材。

在“灵创职业教育·网络与信息安全”系列教材策划过程中,我们组织安全和职教专家对国内目前“网络与信息安全”职教层次人才需求和“网络与信息安全”职教发展现状进行了全面调研分析。研究发现,社会对“网络与信息安全”职教层次的人才需求集中在“信息与网络安全管理”、“安全产品营销与服务”方面。下表显示了对这些岗位职业技能需求和学习领域进行研究分析的结果。

职业目标	岗位主要职责	职业技能要求	学习领域	
			知识	整合课程
信息与网络安全管理	管理、维护操作系统,保障操作系统级安全	1. 系统及应用安全风险评估 2. 系统及应用安全方案设计 3. 系统安全配置 4. 系统安全监控及审计 5. 数据安全 6. 应用系统运行安全	1. 信息安全法规/标准 2. 操作系统访问控制配置 3. 操作系统进程及服务配置 4. 操作系统性能、本地/网络访问监控 5. 系统日志管理 6. 数据备份恢复 7. 漏洞管理 8. 操作系统安全风险分析及工具	1. 信息安全法规与标准 2. 操作系统管理 3. 信息安全导论(操作系统安全部分) 4. 信息安全管理与工程(信息安全风险评估-操作系统)

续表

职业目标	岗位主要职责	职业技能要求	学习领域	
			知识	整合课程
信息与网络安全管理	管理、维护数据库,保障数据库系统安全运行及数据安全	1. 数据库安全风险评估 2. 数据库安全管理方案设计 3. 数据库安全管理	1. 数据库基本概念 2. 数据库基本管理操作 3. 数据库安全管理操作(包括数据库访问控制安全、数据库备份恢复) 4. 数据库安全风险分析及工具	1. 信息安全导论(数据库安全部分) 2. 信息安全管理与工程(信息安全风险评估-数据库)
	管理、维护信息服务,保障信息服务安全运行	1. 安装、配置常见的网络服务 2. 制作网站	1. 常见网络服务器安装、配置、管理 2. 网站制作 3. 网络服务安全	1. 网站制作 2. 网络服务管理与维护 3. 信息安全导论(网络服务安全)
	病毒防护	1. 设计系统计算机病毒防范方案 2. 防毒软件采购 3. 安装和配置计算机病毒软件 4. 防毒软件维护	1. 操作系统原理 2. 计算机病毒原理 3. 防毒软件产品 4. 防毒软件安装、配置、升级管理	1. 计算机病毒防范 2. 信息安全产品与方案
	管理、维护网络,保障网络安全	1. 构建基础网络连接 2. 网络安全风险分析 3. 网络安全方案设计 4. 网络安全设备配置 5. 网络安全监控	1. 网络基础,包括局域网构建、网络协议、常见网络设备交换机、路由器配置管理 2. 网络安全与管理,包括防火墙、VPN、IDS 技术及配置管理基本操作,网络攻击与防护简介 3. 网络攻击与防范,包括各类网络攻击原理,防范手段(如入侵检测、防火墙、VPN 等防范手段的使用)	1. 网络安全与管理 2. 网络攻击与防范技术 3. 信息安全管理与工程(信息安全风险评估-网络安全) * 4. 入侵检测技术 * 5. 防火墙技术 * 6. 黑客防范
	保障物理和环境安全	1. 提出信息系统场地安全需求及建设方案,监控、审计场地安全方案实施情况 2. 提出信息系统自然防灾需求及建设方案,监控和审计防灾方案实施情况 3. 规划设计信息系统物理访问控制方案,监控和审计方案实施情况	1. 电路电工基础 2. 信息系统场地安全、防灾等相关法规、标准 3. 信息系统物理访问控制相关产品	1. 信息安全导论(信息系统物理与环境安全) 2. 信息安全管理与工程 3. 信息安全产品与方案
	信息保密管理	1. 制定信息系统信息保密与数字权益保护方案 2. 采购信息保密、数字权益保护产品 3. 信息保密、数字权益保护方案实施	1. 密码学基础 * 2. 信息隐藏、数字水印、数字权益保护	1. 信息安全导论 2. 信息安全产品与方案(信息隐藏) 3. 信息安全管理与工程(信息保密)
	信息安全工程	1. 设计信息安全体系 2. 采购信息安全产品 3. 管理控制信息安全工程 4. 制定信息安全管理方案	1. 信息安全体系架构 2. 信息安全法规、标准 3. 信息安全管理方案文档编制	1. 信息安全导论 2. 信息安全管理与工程

续表

职业目标	岗位主要职责	职业技能要求	学习领域	
			知识	整合课程
信息与网络安全管理	信息安全策略、信息安全制度制定	1. 分析企业信息系统安全风险 2. 制定全面的安全管理策略和制度	1. 信息安全体系架构 2. 信息安全法规、标准 3. 信息安全管理方案文档编制	1. 信息安全导论(信息安全体系) 2. 信息安全管理与工程(安全管理制度、策略)
	* 行业特色技能: 计算机取证	信息系统取证	1. 信息安全法规 2. 信息系统取证方法、手段与工具使用	* 计算机取证
	* 行业特色技能: 电子商务系统安全	1. 电子商务系统安全方案设计 2. 电子商务系统安全管理维护	1. 电子商务应用基础 2. 网上安全支付系统	* 电子商务安全
安全产品营销与服务	安全产品营销与服务	安全产品营销包括: 1. 客户应用系统的安全风险分析 2. 用户系统安全风险防范方案简单设计 3. 安全产品推介方案、文档策划编写 4. 安全产品演示、讲解 安全产品服务包括: 1. 安全产品安装、使用培训 2. 安全产品故障响应咨询 3. 简易安全产品故障排除	1. 信息及网络安全基础 2. 软件开发基础 3. 硬件开发基础 4. 市场营销 5. 技术支持技巧	1. 信息安全导论 2. 网络安全与管理 3. 信息安全产品与方案 4. 信息安全标准与法规 5. 信息安全产品服务与营销

注: * 为拓展课程

基于以上分析,根据网络与信息安全学科体系的特点,在注重学生的“动手实践和技能专业化”职教原则的指导下,我们选定《信息安全标准与法规》、《网络攻击与防护技术》、《计算机病毒防护》、《网络与信息安全综合实践教程》、《信息安全产品与方案》、《信息安全管理与工程》等作为“灵创职业教育·网络与信息安全”系列教材的首批丛书。

从学科体系角度看,这些教材构成了下图所示网络与信息安全职业教育体系主体:

法 律	技术与开发	管 理
	产品与系统	
	评测与服务	
	使用与集成	
	营销与维护	
	培训与认证	

下表为以上课程教学参考学分。

专业课程名称	建议学分	学分分配	
		讲课	课内实验
信息安全标准与法规	4	2	2
信息安全导论	4	2	2
网络攻击与防护技术	5	3	2
计算机病毒防护	4	2	2
网络安全与管理	5	3	2
网络与信息安全综合实验	4	1	3
信息安全产品与方案	4	2	2
信息安全管理与工程	4	2	2
计算机取证与应急响应	3	2	1
合 计	37	19	18

为确保该套教材的质量,教材编委会由国内著名信息安全专家为主组成,每本教材尽可能由经验丰富的职业教育专家执笔。本套丛书主要定位在开设信息安全类专业的职业院校的教材、相应领域的社会培训教材、从业技术人员自学教材。教材既可适用于全国职业教育信息安全专业学生,又可适用于各类成人自考学生。

本套教材受到了国家 973 项目(2007CB311203,2007CB310704)、教育部高等学校博士学科点专项科研基金资助课题(20070013007,20070013005)、国家自然科学基金与香港研究资助局联合科研基金项目(No. 60731160626)和高等学校学科创新引智计划(No. B08004)的资助,在此特表感谢。

杨义先

教授、博导、长江学者特聘教授

2008 年 3 月

前 言

为了引导高等职业技术学校 and 高等专科学校信息安全相关专业的学生对信息安全产品与方案方面所涉及的知识有一个全面的了解,作者编写了《信息安全产品与方案》这本书。本教材全面地介绍了目前信息安全领域常用的产品与方案,以及信息安全整体解决方案。

在讲解时,可以根据学生对象来选择要教的内容以及内容的深度。对于那些没有学过计算机网络课的学生,可以在课前适当加一些计算机网络、信息安全方面的知识。

本书内容全面,书中内容共 12 章。第 1 章是信息安全与信息安全产品,主要包括信息安全概述、信息安全产品概述、中国信息安全产品测评认证中心介绍。第 2 章是防火墙产品与方案,主要包括防火墙概述、典型的防火墙产品、防火墙的新产品、防火墙产品的选择。第 3 章是入侵检测产品与方案,主要包括入侵检测概述、入侵检测的功能、典型的入侵检测产品、IPS 产品。第 4 章是虚拟专用网络产品与方案,主要包括 VPN 概述、VPN 的特点、典型的 VPN 产品、VPN 产品的选择、VPN 的建设。第 5 章是网络隔离与网闸产品与方案,主要包括网络隔离与网闸概述、网络隔离与网闸的特点、网闸的应用定位、网闸的应用领域、典型的网络隔离与网闸产品、网络隔离与网闸产品的选择。第 6 章是数据备份产品与方案,主要包括数据备份概述、常用的数据备份方式、典型的数据备份产品、数据备份注意事项、个人数据备份的策略。第 7 章是防病毒产品与方案,主要包括防病毒概述、防病毒的作用、典型的防病毒产品、防病毒产品的选择。第 8 章是审计系统产品与方案,主要包括审计系统概述、典型的审计系统产品、安全审计系统产品的选择。第 9 章是安全扫描器产品与方案,主要包括安全扫描器系统概述、安全扫描器系统的作用、典型的安全扫描器产品、安全扫描器产品的选择。第 10 章是反恶意软件产品与方案,主要包括反恶意软件概述、典型的反恶意软件产品、反恶意软件产品的选择。第 11 章是其他信息安全产品与方案,主要包括防水墙、防 DDoS 攻击产品、信息加密产品 PGP、文件恢复工具 Easy Recovery。第 12 章是信息安全整体解决方案,主要包括信息安全整体解决

方案概述、制定信息安全整体解决方案、符合安全标准的安全系统。最后在附录里介绍了一个真实的信息安全整体解决方案。本书第1章由李剑编写,第2章由李剑和李剑勇合写,第3、4、5、6章由李剑编写,第7章由李剑勇编写,第8、9、10、11、12章和附录由李剑编写。除了以上内容之外,书中还介绍了大量的实验和实践内容,以便于学生在学习理论知识的同时进行一些实践性的训练,从而更进一步掌握知识。

感谢北京邮电大学信息安全中心杨义先教授、钮心忻教授、罗群副教授、张茹副教授、崔宝江副教授、谷利泽副教授、李辉副教授、周亚健博士、马兆丰博士、辛阳博士、郑康锋博士、李丽香博士、杨榆博士、张森博士、黄正全博士、郑世慧博士、王励成博士等,他们对本书的出版提出了宝贵的意见和建议。感谢我的博士生导师北京理工大学的曹元大教授,曹老师对于本书的出版给予了极大的支持与帮助。感谢中国电信研究院的赵阳博士、中科院计算技术研究所的谭建龙博士、北京交通大学的姚正林博士,他们对本书的出版给了很大的支持。其他参与本书审阅编写等工作的还有景博、景绍达、白小梅、李胜斌、陈彦侠、益德全、李美丽等这里一并感谢!

本教材也是国家信息产业部重点软课题项目“基于互联网内容安全的关键问题研究”(课题编号:2007-R-103)和国家863课题“IPS、IMS关键技术研究”(课题编号:2005143040)的资助成果。

由于本书作者水平有限,书中疏漏与错误之处在所难免,恳请广大同行和读者指正,我将在下一版中改正。我的电子邮箱是 lijian@bupt.edu.cn。电话(010)86212346。

李 剑

北京邮电大学

目 录

第 1 章 信息安全与信息安全产品概述

1.1 信息安全概述	1
1.1.1 信息安全事件	1
1.1.2 信息安全的概念	2
1.1.3 信息安全的实现目标	2
1.1.4 我国信息安全现状	2
1.2 信息安全产品概述	3
1.2.1 信息安全体系结构与产品	3
1.2.2 我国信息安全产业与产品现状	4
1.2.3 我国信息安全产品市场发展趋势	5
1.2.4 推动国内信息安全产品发展的因素	7
1.3 中国信息安全产品测评认证中心介绍	8
1.3.1 中心简介	8
1.3.2 国家信息安全测评认证体系	8
1.3.3 测评认证项目目录	10
1.3.4 国际测评认证服务组织机构	11
思考题	11

第 2 章 防火墙产品与方案

2.1 防火墙概述	12
2.1.1 防火墙的概念	12
2.1.2 防火墙的作用	13
2.1.3 防火墙的特点	14
2.2 典型的防火墙产品	15
2.2.1 思科公司的 PIX 防火墙	15
2.2.2 CheckPoint 公司的 Firewall-1 防火墙	16
2.2.3 NetScreen 公司的 NetScreen 防火墙	18
2.2.4 天融信网络卫士防火墙	19
2.2.5 联想网御防火墙	20
2.2.6 东软 NetEye 防火墙	21
2.2.7 微软 ISA SERVER 防火墙	22

2.2.8 诺顿个人软件防火墙	24
2.3 防火墙的新产品	26
2.3.1 传统防火墙的局限性	26
2.3.2 分布式防火墙	27
2.4 防火墙的性能指标和功能指标	29
2.4.1 防火墙的性能指标	29
2.4.2 防火墙的功能指标	31
2.5 防火墙产品的选择	34
2.6 防火墙产品实验	36
思考题	37

第3章 入侵检测和入侵防御产品与方案

3.1 入侵检测概述	38
3.2 入侵检测的功能	40
3.3 典型的入侵检测产品	40
3.3.1 Snort 入侵检测系统	40
3.3.2 安氏领信 LinkTrust	43
3.3.3 Enterasys Networks 公司 Dragon Sensor	43
3.3.4 启明星辰天阕入侵检测系统	44
3.3.5 中科网威天眼入侵检测系统	45
3.3.6 中联绿盟冰之眼入侵检测系统	45
3.3.7 入侵检测产品的选择	46
3.4 IPS 产品	48
3.4.1 IPS 概述	48
3.4.2 3Com 公司 H3C 系列 IPS 产品	49
3.4.3 天清入侵防御系统	53
3.5 入侵检测产品的性能指标	54
3.5.1 网络入侵检测系统的指标	54
3.5.2 影响入侵检测系统性能指标的因素	56
3.6 入侵检测产品实验	58
思考题	59

第4章 虚拟专用网络产品与方案

4.1 VPN 概述	60
4.2 VPN 的特点	61
4.3 典型的 VPN 产品	62
4.3.1 思科公司的 VPN 产品	62
4.3.2 华为 3Com VPN	64
4.3.3 联想 VPN 网关	65

4.3.4 天融信网络卫士 VPN	66
4.3.5 亿阳公司 VPN 产品	68
4.4 VPN 产品的选择	68
4.5 VPN 的建设	69
4.5.1 自建还是外包	69
4.5.2 选用 VPN 方案时应注意的问题	70
4.5.3 构建端到端安全 VPN 应包含的组成部分	71
4.6 VPN 产品的性能指标	72
4.7 VPN 产品实验	72
思考题	73

第 5 章 网络隔离与网闸产品与方案

5.1 网络隔离与网闸概述	74
5.1.1 物理安全隔离卡	74
5.1.2 其他物理隔离设备	76
5.2 网络隔离与网闸的特点	77
5.3 网闸的应用定位	78
5.4 网闸的应用领域	79
5.5 典型的网络隔离与网闸产品	80
5.5.1 中网公司的网闸产品 X-GAP	80
5.5.2 鲸鱼通信公司的网闸 e-Gap	83
5.5.3 矛头公司的网闸 NetGAP	84
5.5.4 天行网安公司的网闸 Topwalk-GAP	85
5.5.5 伟思公司的网闸 ViGap	85
5.5.6 联想网御 SIS-3000 安全隔离与信息交换系统	86
5.6 网络隔离与网闸产品的性能指标	89
5.7 网络隔离与网闸产品的选择	89
5.8 网络隔离与网闸产品实验	90
思考题	91

第 6 章 数据备份产品与方案

6.1 数据备份概述	92
6.2 常用的数据备份方式	94
6.3 典型的数据备份产品	95
6.3.1 VERITAS 公司数据备份产品	95
6.3.2 Legato NetWorker	95
6.3.3 CA 公司的 ARCserve	97
6.3.4 赛门铁克公司的 Ghost	98
6.3.5 PowerQuest 公司的 Drive Image	102

6.3.6 北京和力记易科技有限公司的 UPM 数据库保镖	102
6.4 数据备份注意事项	105
6.5 个人数据备份的策略	106
6.6 数据备份产品实验	107
思考题	108

第 7 章 防病毒产品与方案

7.1 防病毒概述	109
7.2 防病毒的作用	109
7.3 典型的防病毒产品	110
7.3.1 诺顿杀毒软件	110
7.3.2 McAfee VirusScan	121
7.3.3 Pc-cillin 杀毒专家	125
7.3.4 卡巴斯基反计算机病毒软件	125
7.3.5 瑞星杀毒软件	126
7.3.6 江民 KV 杀毒软件	130
7.3.7 金山毒霸	131
7.3.8 熊猫卫士	131
7.4 防病毒产品性能比较	131
7.5 防病毒产品的选择	132
7.6 防病毒产品实验	132
思考题	133

第 8 章 审计系统产品与方案

8.1 审计系统概述	134
8.2 典型的审计系统产品	135
8.2.1 天融信的 TA 安全审计综合分析系统	135
8.2.2 捷普安全审计系统	136
8.2.3 启明星辰天玥网络安全审计系统	138
8.2.4 剑鱼网络安全监控审计系统	139
8.2.5 冠群金辰 eTrust Audit 日志审计系统	140
8.2.6 国卫博达	140
8.2.7 二零盛安鹰眼网络安全审计系统	141
8.3 安全审计系统产品的选择	143
8.4 审计系统实验	143
思考题	144

第 9 章 安全扫描器产品与方案

9.1 安全扫描器系统概述	145
---------------------	-----

9.2 安全扫描器系统的作用	147
9.3 典型的安全扫描器产品	147
9.3.1 SSS	148
9.3.2 流光扫描器	151
9.3.3 N-Stalker Web 扫描器	152
9.3.4 Nessus 安全扫描器	154
9.3.5 Nmap 扫描器	155
9.3.6 启明星辰天镜脆弱性扫描与管理系统	156
9.4 安全扫描器产品的选择	157
9.5 安全扫描器系统实验	158
思考题	159
第 10 章 反恶意软件产品与方案	
10.1 反恶意软件概述	160
10.2 典型的反恶意软件产品	161
10.2.1 奇虎 360 安全卫士	162
10.2.2 超级兔子清理王	165
10.2.3 IE 插件管理专家 Upiea	167
10.2.4 恶意软件清理助手	168
10.3 反恶意软件产品的选择	169
思考题	169
第 11 章 其他信息安全产品与方案	
11.1 防水墙	170
11.1.1 防水墙概述	170
11.1.2 中软 WaterBox 防水墙系统	171
11.1.3 雨人防水墙产品	172
11.2 防 DDoS 攻击产品	174
11.2.1 绿盟黑洞防 DDoS 产品	175
11.2.2 方正黑鲨防 DDoS 产品	177
11.3 信息加密产品 PGP	179
11.3.1 PGP 简介	179
11.3.2 PGP 的使用	180
11.4 文件恢复工具 Easy Recovery	182
11.4.1 Easy Recovery 简介	182
11.4.2 Easy Recovery 使用	183
思考题	184

第 12 章 信息安全整体解决方案

12.1 制定信息安全整体解决方案.....	185
12.1.1 应遵循的原则.....	185
12.1.2 注意事项.....	186
12.1.3 制定信息安全整体解决方案具体内容.....	187
12.1.4 实例.....	188
12.2 符合安全标准的安全系统.....	188
思考题.....	189
附录 北京某公司安全整体解决方案.....	190
参考文献.....	203