

安博教育集团职业教育标准教材

网络安全基础

安博教育集团 编著

网络
方向



电子工业出版社

PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

<http://www.phei.com.cn>

安博教育集团职业教育标准教材

网络安全基础

安博教育集团 编著

電子工業出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

本书分为网络安全基础, ISA2006 两大部分。内容包括: 计算机网络安全概述; 黑客攻击技术介绍; 操作系统安全; 网络安全管理; 路由器和交换机网络安全; 身份认证技术; 防火墙, 入侵检测技术介绍; VPN 技术; ISA 概述; 安装与部署 ISA Server 2006; ISA Server 客户端的部署; 配置网页缓存; 控制内网访问 Internet; 通过 ISA 发布内部站点, 邮件服务及其他各类服务; 配置入侵检测。

本书内容新颖, 编辑合理, 论述清晰, 不仅适合用做计算机职业培训的首选教材, 也适合普通高校学生作为教材使用。

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。

图书在版编目 (CIP) 数据

网络安全基础 / 安博教育集团编著. —北京: 电子工业出版社, 2012.2

安博教育集团职业教育标准教材

ISBN 978-7-121-15155-2

I. ①网… II. ①安… III. ①计算机网络—安全技术—职业教育—教材 IV. ①TP393.08

中国版本图书馆 CIP 数据核字 (2011) 第 236712 号

策划编辑: 关雅莉

责任编辑: 郝黎明 文字编辑: 裴 杰

印 刷: 三河市鑫金马印装有限公司

装 订:

出版发行: 电子工业出版社

北京市海淀区万寿路 173 信箱 邮编 100036

开 本: 787×1092 1/16 印张: 29.5 字数: 755.2 千字 彩插: 1

印 次: 2012 年 2 月第 1 次印刷

定 价: 81.00 元

凡所购买电子工业出版社图书有缺损问题, 请向购买书店调换。若书店售缺, 请与本社发行部联系, 联系及邮购电话: (010) 88254888。

质量投诉请发邮件至 zlt@phei.com.cn, 盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线: (010) 88258888。

安博教育集团 (NYSE:AMBO)



安博教育是“以学习者为中心”面向个人及机构提供学习和教育服务的领航机构，业务涉及基础教育服务、职业教育服务、企业培训等领域，以重点解决升学和就业两大关键需求为目标，为各个阶段学习者提供高效的个性化学习服务。

2010年8月5日，安博教育成功登陆美国纽交所。

安博对中国教育市场有着深刻理解，并且是国内少数拥有丰厚技术优势的教育公司，安博真正把传统教育资源、网络技术资源与个体教育需求整合了起来，并已形成规模，领导了中国教育服务发展的方向。

安博教育官网：www.ambow.com

安博职业教育



安博职业教育机构分布图

安博职业教育运营集团隶属于安博教育集团，致力于为大学生提供最专业的就业服务。

就内容来讲，安博教育集团IT职业教育提供软件工程、网络工程、动漫设计、服务外包12个专业方向4大系列课程，同时包括职业素养类课程和国际合作项目，与全球IT软件、网络、服务外包和动漫设计领域的技术发展同步，通过安博独特的IT实训人才培养模式，从专业技能、项目能力和职业素质三方面帮助广大学员全面提升职场就业竞争力、快速成为“到岗就能胜任工作”的复合型、实用型人才。

除了在全国建立自己的直营院校和培训机构，安博还建立了全国最大的园区型实训基地，以及覆盖总部、分支机构、各直营院校、实训基地的IT基础设施网络平台，包括IT实训平台、就业导航平台等。

安博实训平台

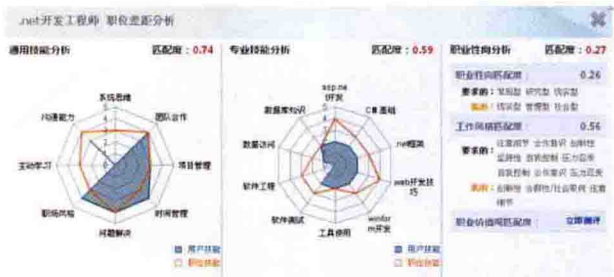
实训平台依托安博丰富的项目开发实践和人才实训经验，结合软件工程思想和计算机辅助技术，加入大量的资源内容，为院校提供人才实训服务。



安博实训平台界面截图

安博就业导航平台

就业导航平台是教育培训领域的创新应用，旨在为初入职场的人员（包括大学毕业生群体）提供就业能力的测评、提升以及求职服务。



安博就业导航平台-胜任力模型图

1 安博（昆山）服务外包产业园



基地效果图

安博（昆山）服务外包产业园由昆山花桥经济开发区和安博教育集团共同建设和运营，总投资逾4亿元。园区占地120亩，建筑面积11万平方米，同期容量超过5000人，是国内第一个园区型实训基地。

依托长三角的产业优势，整合IBM、HP、Microsoft、Adobe、Cisco等国际权威IT厂商、服务外包厂商的企业资源及国内外知名高校和教育机构的教育资源，昆山实训基地开展了国际职业人才实训与就业推荐、国际人才输出、人力资源服务与派遣、承接软件服务外包项目，为加强上海、江苏以及周边地区核心竞争力提供了充沛的智力与人才支撑，进而实现“区域教育服务区域经济”的目标。

1 安博（大连）软件与服务外包人才实训基地

安博（大连）软件与服务外包人才实训基地由大连高新区政府与安博教育集团共同建设和运营，总投资6亿元。基地占地11公顷，建筑面积20余万平方米，设置了企业区、实训区、生活区和人才会展中心四大功能区域，可以同时容纳1万人实训，是目前国内最大、最专业的园区型IT实训基地。

依托大连及环渤海产业优势，大连实训基地将开展IT人才实训、订单培养、企业人才培养、IT人才派遣以及国际国内高级项目经理培训等业务，每年将为大连输送2万余名合格的软件与服务外包人才，为大连建设全球软件和服务外包新领军城市提供智力与人才支撑。



基地全景



1 安博广州实训基地



基地效果图

安博广州实训基地秉承安博“区域教育服务区域经济”的指导纲领，以广州为核心点，将建设成大规模的集实训区、生活区、企业区以及人才会展中心等功能为一体的分布式实训基地。

基地将充分发挥珠江三角洲地区的政治、经济、文化优势，将安博教育集团的技术、资本、平台优势与区域环境和产业优势相结合，大力提升所在区域招商引资方面的人才储备能力，实现产业需求与政府导向的无缝链接。

未来广州基地将成为面向全国的人才、项目、企业三大资源汇聚地。

序言

百年大计，教育为本。教育是民族振兴、社会进步的基石，是提高国民素质、促进人的全面发展的根本途径，寄托着亿万家庭对美好生活的期盼。2010年7月，国务院颁发《国家中长期教育改革和发展规划纲要（2010—2020）》。这份《纲要》把“坚持能力为重”放在了战略主题的位置，指出教育要“优化知识结构，丰富社会实践，强化能力培养。着力提高学生的学习能力、实践能力、创新能力，教育学生学会知识技能，学会动手动脑，学会生存生活，学会做人做事，促进学生主动适应社会，开创美好未来。”这对学生的职前教育、职后培训都提出了更高的要求，需要建立和完善多层次、高质量的职业培养机制。

安博教育集团率先倡导“构建中国自己的开放式网络教育平台”，并最早实践、研创出教育部鉴定并符合国际标准的网络教育平台；同时，安博是全国信息技术标准化委员会教育技术分技术委员会的核心创建成员，是国际化软件工程高级人才培养体系、实训体系、园区型实训基地的倡导者和最早实践者。

当前，作为国内教育培训业内最大的整合者，安博教育的优势主要集中在三个方面：一是安博在通过信息化手段与教育的结合方面有着独特的理解和成功尝试。此外安博对中国教育市场有深刻理解，并且是国内少数拥有丰厚技术优势的教育公司。安博能充分整合来自国际厂商和企业人才的需求，并将传统教育资源、先进的行业技术资源与学习者的个性化需求进行有机的结合，实现了真正意义上的“教育是满足企业和行业发展需求”的终极目标。二是拥有遍布全国的实施网络和大型基地，以及大量具备企业项目实施经验和教育培训经验的优秀教师，通过高品质标准化的教育服务为其业务稳步发展起到了重要保障和促进作用。三是安博受到国家教育部及各地教育部门的大力支持和高度认可，安博是教育部IT实训推广工程的唯一实施单位。

安博教育服务业务以重点解决升学和就业两大关键需求为目标，为各个阶段学习者提供高效的个性化学习服务。目前，安博教育集团的业务涉及基础教育服务、职业教育服务、企业培训等领域，基地、学校、机构等已遍及全国数十个重点城市，形成了以区域教育服务中心和实训基地为依托，以师资、课程、服务流程、IT支持、网络学习服务的标准化为载体的服务体系，通过标准品质的服务保障全国各地用户的个性化需求。



为了贯彻落实党中央、国务院关于大力发展高等职业教育、培养高等技术应用型人才的战略部署，解决高职高专院校缺乏实用性教材的问题，安博根据企业工作岗位要求和院校的教学需要，充分汲取高职高专院校在探索培养高等技术应用型人才方面取得的成功经验和教学成果，并依托安博丰厚的 IT 产业背景，坚持自主研发和强强合作的指导思想，组织编写了本套“职业教育标准教材”丛书。

在组织编写中，我们力求使这套教材具有以下特点。一是根据国内产业经济发展现状，加大课程体系、实训体系及自主知识产权软件产品的研发力度；二是积极引进国际先进的课程与技能资源，大力推动国际合作，实现安博教育体系与国际教育体系的接轨，实现课程无缝对接与学分互认；三是从职业（岗位）分析入手，围绕课程的教学目标，体现技能训练的针对性；四是突出教材的先进性，更多地将新技术融入其中，以期缩短学校教育与企业需要的距离，更好地满足企业用人的需要；五是贯彻以技能训练为主线、相关知识为支撑的编写思路，切实落实“管用、够用、适用”的教学指导思想。

此次出版的职业教育标准教材，是安博实训理念探索和实践的又一步，我们希望能为提升大学生的就业竞争力和就业质量尽自己的绵薄之力。

“红日初升，其道大光；河出伏流，一泻汪洋。”新的征程已经开始，安博职教将继续前行，争做中国最专业的的大学生就业服务提供商！

安博职业教育运营集团 总裁
编审委员会 主席

前言

本套教材在保证知识体系完备，脉络清晰，论述精准深刻的同时，尤其注重培养读者的实际动手能力和企业岗位技能的应用能力，并结合大量的工程案例和项目来使读者更进一步灵活掌握及应用相关的技能。

本书内容

全书共分为 18 章，内容由浅入深，全面覆盖了网络安全的基础知识及相关技术。

第 1 章，讲解网络安全的现状和发展趋势，并对网络的主流攻击有了初步认识。

第 2 章，讲解网络主流攻击的原理，也了解了常用的攻击软件的特点。

第 3 章，讲解 Windows 系统的发展史和安全性优化思路，以及 Linux/UNIX 的安全性优化思路。

第 4 章，讲解网络安全管理的重要性，及详细讲解 SNMP 协议。

第 5 章，讲解路由器，交换机的安全优化思路。

第 6 章，讲解身份认证技术的分类，应用和发展趋势。

第 7 章，讲解防火墙功能，分类及访问控制列表的分类配置。

第 8 章，讲解入侵检测系统的原理，发展和选型。

第 9 章，讲解 VPN 技术的原理、VPN 技术的隧道概念、VPN 的分类和层次，以及 IPsec 和 SSL VPN 技术。

第 10 章，讲解 ISA Server 2006 的基本知识，阐述了 ISA Server 的三方面功能。

第 11 章，本章主要介绍了 ISA Server 2006 的安装过程和部署方法。

第 12 章，本章主要讲如何使用 ISA 2006 的三种客户端。

第 13 章，本章介绍了 ISA Server 2006 在网页加速方面的使用方法。

第 14 章，本章主要介绍了如何控制内网用户访问 Internet 的网络资源。

第 15 章，本章主要介绍了使用 ISA Server 2006 发布内部站点的方法。

第 16 章，本章介绍了使用 ISA Server 2006 发布邮件服务器的方法。

第 17 章，本章主要介绍了发布其他类型服务器的方法，并且介绍了使用 ISA Server 2006 制定规则的注意事项。

第 18 章，本章介绍了 ISA Server 2006 具备的入侵检测的功能。

配套教学资源

本书提供了配套的立体化教学资源，包括教学大纲、电子教案、源代码、项目案例等配套文档以及素材库等必需的文件，读者可以通过华信教育资源网（www.hxedu.com.cn）下载使用。



本书主编

本书由张泽飞、谢湘豫、张航主编。由于作者水平有限，错漏之处在所难免，请广大读者批评指正。

特别鸣谢

特别鸣谢安博亚威科技（北京）对本书编写工作的大力支持，并同时鸣谢安博（大连）软件和服务外包人才实训基地、安博（昆山）服务外包人才实训基地、安博华南实训基地、安博广州金桥学校、安博大连希望学校、安博上海英豪学院、安博天津数字艺术产业基地、安博中程在线（北京）、安博长沙牛耳学校、安博河北实训基地、安博山东师创学院、安博西南实训基地的学术研究团队对本书进行了认真的审校及建议。

主 编

2011年9月

读者意见反馈表

个人资料

姓名_____ 年龄_____ 联系电话_____ (办)_____ (宅)_____ (手机)_____
学校_____ 专业_____ 职称/职务_____
通信地址_____ 邮编_____ E-mail_____

您校开设课程的情况为:

本校是否开设相关专业的课程 是, 课程名称为_____ 否
您所讲授的课程是_____ 课时_____
所用教材_____ 出版单位_____ 印刷册数_____

本书可否作为您校的教材?

是, 会用于_____ 课程教学 否

影响您选定教材的因素(可复选):

内容 作者 封面设计 教材页码 价格 出版社
是否获奖 上级要求 广告 其他_____

您对本书质量满意的方面有(可复选):

内容 封面设计 价格 版式设计 其他_____

您希望本书在哪些方面加以改进?

内容 篇幅结构 封面设计 增加配套教材 价格

可详细填写: _____

您还希望得到哪些专业方向教材的出版信息?

感谢您的配合, 可将本表按以下方式反馈给我们:

【方式一】电子邮件: 登录华信教育资源网 (http://www.hxedu.com.cn/resource/OS/zixun/zz_reader.rar) 下载本表格电子版, 填写后发至 gaozhi@phei.com.cn

【方式二】邮局邮寄: 北京市万寿路 173 信箱华信大厦 1101 室 职业教育分社 (邮编: 100036)

反侵权盗版声明

电子工业出版社依法对本作品享有专有出版权。任何未经权利人书面许可，复制、销售或通过信息网络传播本作品的行为；歪曲、篡改、剽窃本作品的行为，均违反《中华人民共和国著作权法》，其行为人应承担相应的民事责任和行政责任，构成犯罪的，将被依法追究刑事责任。

为了维护市场秩序，保护权利人的合法权益，我社将依法查处和打击侵权盗版的单位和个人。欢迎社会各界人士积极举报侵权盗版行为，本社将奖励举报有功人员，并保证举报人的信息不被泄露。

举报电话：(010) 88254396；(010) 88258888

传 真：(010) 88254397

E-mail: dbqq@phei.com.cn

通信地址：北京市海淀区万寿路 173 信箱

电子工业出版社总编办公室

邮 编：100036

目录

第一部分 网络安全技术

第 1 章 计算机网络安全概述	(3)
1.1 网络安全简介	(4)
1.1.1 网络安全的发展	(4)
1.1.2 网络安全的定义和重要性	(7)
1.2 网络安全弱点和主流的网络攻击简介	(10)
本章小结	(13)
习题	(13)
第 2 章 黑客攻击技术介绍	(15)
2.1 扫描探测	(16)
2.1.1 扫描器攻击介绍	(16)
2.1.2 扫描技术的分类	(16)
2.1.3 扫描器主流软件介绍	(17)
2.2 嗅探侦听	(19)
2.2.1 网络侦听原理	(19)
2.2.2 Sniffer 工具的介绍和使用	(20)
2.3 缓冲区溢出攻击	(25)
2.4 拒绝服务与分布式拒绝服务	(26)
2.4.1 DoS 攻击介绍	(26)
2.4.2 DDoS 攻击介绍	(27)
2.4.3 DoS/DDoS 攻击的具体表现	(27)
2.4.4 常见的 DoS/DDoS 攻击	(28)
2.4.5 如何防止 DoS/DDoS 攻击	(30)
2.5 病毒	(31)
2.5.1 病毒定义	(31)
2.5.2 病毒的分类	(32)
2.5.3 计算机病毒的防治	(36)
2.6 木马	(39)
2.6.1 木马的工作原理	(39)
2.6.2 木马的隐藏与检测	(40)



2.6.3 木马的查杀	(42)
2.6.4 木马的防护	(43)
2.7 智能安全网络架构	(43)
2.7.1 智能安全网络架构的组成	(43)
2.7.2 虚拟专用网 VPN 技术	(43)
2.7.3 防火墙系统	(44)
2.7.4 入侵检测系统	(46)
2.7.5 网络访问控制和健康状态审查	(47)
本章小结	(49)
习题	(49)

第 3 章 操作系统安全

3.1 操作系统安全对比	(52)
3.2 Windows 操作系统	(53)
3.2.1 Windows 操作系统简介	(53)
3.2.2 Windows 家族	(53)
3.2.3 Windows 系统安全管理	(62)
3.2.4 Windows 系统安全实施模板	(68)
3.3 Linux/UNIX 系统安全	(73)
3.3.1 Linux 简介	(73)
3.3.2 UNIX 简介	(74)
3.3.3 Linux/UNIX 系统安全管理	(74)
本章小结	(78)
习题	(78)

第 4 章 网络安全管理

4.1 网络管理技术概述	(80)
4.2 网络安全管理现状与需求	(80)
4.3 网络安全管理技术及功能简介	(81)
4.4 安全管理的发展现状	(82)
4.5 SNMP 协议	(82)
4.5.1 SNMP 协议介绍	(82)
4.5.2 SNMP 的命令和报文	(83)
4.5.3 管理信息数据库	(84)
4.5.4 SNMP 的发展	(85)

本章小结	(86)
习题	(86)
第5章 路由器和交换机网络安全	(87)
5.1 路由器安全概述	(88)
5.1.1 路由器扮演安全角色	(88)
5.1.2 路由器的安全初试	(89)
5.1.3 路由器安全优化要点	(90)
5.1.4 多级管理	(99)
5.1.5 安全登录控制	(103)
5.2 路由器安全管理	(105)
5.2.1 syslog 日志	(105)
5.2.2 NTP 网络设备间的时间同步	(107)
5.2.3 SSH 安全远程管理	(107)
5.3 交换机网络安全	(109)
5.3.1 虚拟局域网	(109)
5.3.2 三层交换技术	(114)
5.3.3 端口安全	(114)
5.3.4 端口流量控制	(116)
5.3.5 网络访问控制与 802.1x 认证	(118)
5.3.6 DHCP 侦听	(124)
5.3.7 DAI (动态 ARP 检测)	(126)
本章小结	(128)
习题	(128)
第6章 身份认证技术	(129)
6.1 身份认证技术简介	(130)
6.2 身份认证技术分类	(130)
6.3 身份认证技术发展趋势	(131)
6.4 生物识别	(132)
6.4.1 生物识别技术概念	(132)
6.4.2 几种常见的生物特征识别方式	(133)
6.4.3 生物特征识别技术在中国的发展状况	(135)
6.5 指纹认证	(136)
6.6 虹膜识别技术	(138)



6.6.1 虹膜作为身份标识具有许多先天优势	(138)
6.6.2 虹膜识别过程	(139)
6.7 数字认证	(141)
本章小结	(142)
习题	(142)

第7章 防火墙技术介绍

7.1 认识防火墙	(144)
7.1.1 什么是防火墙	(144)
7.1.2 防火墙的功能	(145)
7.1.3 防火墙的分类	(148)
7.1.4 防火墙的优缺点比较	(152)
7.2 包过滤型防火墙	(153)
7.2.1 包过滤型防火墙的工作原理	(153)
7.2.2 访问控制列表	(154)
7.2.3 标准 ACL	(155)
7.2.4 扩展 ACL	(157)
7.2.5 命名的 ACL	(158)
7.2.6 ACL 注释	(158)
7.2.7 基于时间的 ACL	(159)
7.2.8 自反 ACL	(159)
7.2.9 动态 ACL (锁和密钥)	(162)
7.2.10 Turbo ACL	(164)
7.3 状态检测型防火墙	(165)
7.3.1 状态检测型防火墙的工作原理	(165)
7.3.2 状态检测型防火墙产品介绍	(167)
本章小结	(168)
习题	(169)

第8章 入侵检测技术

8.1 入侵检测系统概述	(172)
8.2 入侵检测系统发展史	(173)
8.3 入侵检测系统的分类和对比	(176)
8.3.1 入侵检测系统的分类	(176)
8.3.2 入侵检测系统的对比	(178)
8.4 入侵检测的检测算法	(179)

8.5 入侵检测系统算法特征	(180)
8.6 入侵检测结构	(181)
8.7 入侵检测系统的演进	(182)
8.8 入侵检测产品和市场分析	(183)
8.8.1 入侵检测产品	(183)
8.8.2 入侵检测系统市场分析	(186)
本章小结	(187)
习题	(187)
第9章 VPN 技术	(189)
9.1 VPN 技术概述	(190)
9.1.1 VPN 技术的企业应用	(190)
9.1.2 VPN 的实现方式	(190)
9.1.3 VPN 技术的需求	(191)
9.1.4 VPN 的隧道概念	(192)
9.1.5 VPN 隧道技术的实现	(192)
9.1.6 PPP 拨号会话过程	(194)
9.1.7 VPN 的隧道技术分类	(195)
9.2 通用路由封装协议 GRE	(200)
9.3 IPSec 介绍	(205)
9.3.1 IPSec 安全特性	(205)
9.3.2 IPSec 技术特点和组成	(206)
9.3.3 对称加密	(207)
9.3.4 非对称加密	(208)
9.3.5 数据完整性 HMAC	(208)
9.3.6 Diffie-Hellman 密钥交换协议	(209)
9.3.7 源验证方式介绍	(209)
9.3.8 IPSec VPN 应用范例	(210)
9.4 SSL 虚拟专用网技术	(215)
9.4.1 SSL 基础	(216)
9.4.2 SSL 通信的工作原理	(217)
9.4.3 SSL VPN 的主要优点和不足	(218)
9.4.4 SSL VPN 配置应用范例	(220)
本章小结	(224)
习题	(224)



第二部分 ISA 2006

第 10 章 ISA 概述	(227)
10.1 防火墙概述	(228)
10.1.1 软件防火墙	(228)
10.1.2 硬件防火墙	(228)
10.1.3 防火墙的特点	(229)
10.1.4 防火墙的功能	(229)
10.2 ISA Server 2006 功能概述	(230)
10.3 ISA Server 2006 加速 Web 访问	(231)
10.4 防火墙的设置种类	(233)
10.5 ISA Server 与 VPN 的集成	(236)
本章小结	(237)
习题	(237)
第 11 章 安装与部署 ISA Server 2006	(239)
11.1 ISA Server 2006 企业版的特点	(240)
11.2 ISA Server 部署与使用注意事项	(240)
11.2.1 安装 ISA Server 的软件需求	(240)
11.2.2 安装 ISA Server 的硬件环境	(241)
11.2.3 ISA Server 的安装	(241)
11.2.4 无人值守安装	(253)
11.3 ISA Server 的部署位置	(255)
11.3.1 Internet 边缘防火墙	(256)
11.3.2 部门或主干网络防火墙	(256)
11.3.3 分支办公室防火墙	(256)
11.3.4 安全服务器发布	(257)
11.3.5 角色管理	(257)
11.4 测试 ISA Server 防火墙是否安装成功	(260)
11.4.1 打开 ISA Server 管理工具	(260)
11.4.2 防火墙阻挡测试	(261)
11.4.3 开放服务器访问外网网页	(262)
本章小结	(266)
习题	(266)