

<<网络安全基础教程与实训>>

图书基本信息

书名：<<网络安全基础教程与实训>>

13位ISBN编号：9787301096673

10位ISBN编号：7301096674

出版时间：2005-9

出版时间：北京大学出版社

作者：杨诚

页数：297

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<网络安全基础教程与实训>>

前言

北京大学出版社第六事业部组编了一套《21世纪全国高职高专计算机系列实用规划教材》。

为此,制订了详细的编写目的、丛书特色、内容要求和风格规范。

在内容上强调面向职业、项目驱动、注重实例、培养能力;在风格上力求文字精练、图表丰富、脉络清晰、版式明快。

一、组编过程2004年10月,第六事业部开始策划这套丛书,分派编辑深入各地职业院校,了解教学第一线的情况,物色经验丰富的作者。

2005年1月15日在济南召开了“北大出版社高职高专计算机规划教材研讨会”。

来自13个省、41所院校的70多位教师汇聚一堂,共同商讨未来高职高专计算机教材建设的思路和方法,并对规划教材进行了讨论与分工。

2005年6月13日在苏州又召开了“高职高专计算机教材大纲和初稿审定会”。

编审委员会委员和45个选题的主、参编,共52位教师参加了会议。

审稿会分为公共基础课、计算机软件技术专业、计算机网络技术专业、计算机应用技术专业4个小组对稿件逐一进行审核。

力争编写出一套高质量的、符合职业教育特点的精品教材。

二、知识结构职业生涯的成功与人们的知识结构有关。

以著名侦探福尔摩斯为例,作家柯南道尔在“血字的研究”中,对其知识结构描述如下:文学知识--无;哲学知识--无;政治学知识--浅薄;植物学知识--不全面。

对于药物制剂和鸦片却知之甚详。

对毒剂有一般了解,而对于实用园艺却一无所知;化学知识--精深;地质学知识--偏于应用,但也有限。

他一眼就能分辨出不同的土质。

根据裤子上泥点的颜色和坚实程度就能说明是在伦敦什么地方溅上的;解剖学知识--准确,却不系统;惊险小说知识--很渊博。

似乎对近一个世纪发生的一切恐怖事件都深知底细;法律知识_一熟悉英国法律,并能充分实用;其他--提琴拉得很好,精于拳术、剑术。

事实上,我国唐朝名臣狄仁杰,大宋提刑官宋慈,都有类似的知识结构。

审视我们自己,每人的知识结构都是按自己的职业而建构的。

因此,我们必须面向,职场需要来设计教材。

<<网络安全基础教程与实训>>

内容概要

网络安全基础知识是网络安全教育和培训过程中首先要学习和掌握的内容，本教材全面介绍了网络安全的基本框架、网络安全的基本理论以及计算机网络安全方面的管理、配置和维护。

全书共分10章，主要内容包括：网络安全概述、IP数据报结构、密码技术、Windows 2000系统安全、病毒分析与防御、应用服务安全、网络攻击与防范、VPN技术、防火墙技术、入侵检测系统。

本教材注重实践技能的培养，以实训为依托，深入浅出地讲解理论知识，因此既可作为高职高专院校计算机及相关专业的学生教材，也可作为计算机网络安全类的技术参考书或培训教材。

<<网络安全基础教程与实训>>

书籍目录

第1章网络安全概论1.1网络安全概念1.1.1网络安全的概念1.1.2网络安全的现状1.2网络安全所产生的威胁1.2.1网络中存在的威胁1.2.2主机网络安全1.2.3主机网络安全系统体系结构1.3协议安全分析1.3.1物理层安全1.3.2网络层安全1.3.3传输层安全1.3.4应用层安全1.4网络安全标准1.4.1国外网络安全标准与政策现状1.4.2ISO7498-2安全标准1.4.3BS7799(ISO17799:2000)标准1.4.4国内安全标准、政策制定和实施情况1.5网络安全组件1.6安全策略的制定与实施1.6.1安全工作目的1.6.2安全策略1.6.3安全策略的实施1.7本章习题第2章IP数据报结构2.1流量监控与数据分析2.1.1局域网数据流量的监控2.1.2Sniffer工具介绍2.1.3深入了解Sniffer2.2网络层协议报头结构2.2.1IP2.2.2ARP2.2.3ICMP2.2.4IGMP2.3传输层协议报头结构2.3.1TCP2.3.2UDP2.4TCP会话安全2.5数据流捕捉与分析2.5.1捕获过程报文统计2.5.2捕获报文查看2.5.3设置捕获条件2.5.4ARP报文解码2.5.5IP报文解码2.6本章实训实训:使用Sniffer工具进行捕获分析2.7本章习题第3章密码技术3.1对称密码体制3.1.1对称加密体制的概念3.1.2DES算法3.1.3DES算法实现3.2公钥密码体制3.2.1公钥密码体制的概念3.2.2RSA算法3.2.3RSA算法实现3.3数字签名技术3.3.1数字签名技术的概念3.3.2数字签名的实现方法3.3.3数字签名的其他问题3.4密钥管理3.4.1私钥分配3.4.2公钥分配3.4.3用公钥加密分配私钥密码体制的密钥3.5认证3.5.1身份认证3.5.2主机之间的认证3.5.3Kerberos认证3.6本章实训实训:SSH安全认证3.7本章习题第4章Windows2000系统安全4.1操作系统安全基础4.1.1安全管理目标4.1.2安全管理措施4.2Windows2000账号安全4.2.1账号种类4.2.2账号与密码约定4.2.3账号和密码安全设置4.3Windows2000文件系统安全4.3.1NTFS权限及使用原则4.3.2NtFS权限的继承性4.3.3共享文件夹权限管理4.3.4文件的加密与解密4.4Windows2000主机安全4.4.1使用安全策略4.4.2设置系统资源审核4.5本章实训实训:组策略配置实训2:文件系统安全实训3:主机安全4.6本章习题第5章病毒分析与防御5.1计算机病毒概述5.1.1计算机病毒产生发展的历史5.1.2计算机病毒的定义5.1.3计算机病毒的产生原因及来源5.1.4计算机病毒的特性5.1.5计算机病毒的分类5.1.6计算机病毒感染的表现5.2病毒机制与组成结构5.2.1计算机病毒的组成结构5.2.2计算机病毒的传染5.2.3计算机病毒的触发机制5.2.4计算机病毒的生存周期5.3病毒实例剖析5.3.1Nimda蠕虫病毒剖析5.3.2CodeRedII剖析5.3.3CIH病毒5.4病毒的防范与清除5.4.1防范病毒5.4.2检测病毒5.4.3清除病毒5.5病毒和反病毒的发展趋势5.5.1病毒的发展趋势5.5.2病毒清除技术的发展趋势5.5.3防病毒系统的要求5.6本章实训实训:病毒代码特征分析实训2:防病毒软件应用5.7本章习题第6章应用服务安全6.1应用服务概述6.1.1客户机/服务器模型6.1.2应用服务的划分6.1.3Internet的安全6.2Web服务的安全6.2.1IIS.Web安全设置6.2.2浏览器的安全性6.3FTP服务的安全6.3.1目录安全设置6.3.2用户验证控制6.3.3IP地址限制访问6.3.4其他安全措施6.4电子邮件服务的安全6.4.1E-mail工作原理及安全漏洞6.4.2安全风险6.4.3安全措施6.4.4IIS-SMTP服务安全6.4.5OutlookExpress安全6.5SQLServer2000安全6.5.1身份认证模式6.5.2安全配置6.6本章实训实训1:Web服务安全实训2:FTP服务安全实训3:电子邮件服务安全6.7本章习题第7章防火墙技术7.1防火墙概述7.1.1防火墙的定义7.1.2防火墙的发展7.2防火墙的功能7.2.1防火墙的访问控制功能7.2.2防火墙的防止外部攻击7.2.3防火墙的地址转换7.2.4防火墙的日志与报警7.2.5防火墙的身份认证7.3防火墙技术7.3.1防火墙的包过滤技术7.3.2防火墙的应用代理技术7.3.3防火墙的状态检测技术7.3.4防火墙系统体系结构7.3.5防火墙的主要技术指标7.4防火墙的不足7.5防火墙产品介绍7.5.1Cisco防火墙简介7.5.2NetST防火墙简介7.6防火墙应用典型案例7.6.1背景描述7.6.2系统规划7.6.3功能配置7.7本章实训实训1:防火墙配置实训2:Windows2000自身IP安全策略7.8本章习题第8章入侵检测系统8.1入侵检测系统概述8.1.1入侵检测定义8.1.2入侵检测系统的主要功能8.2入侵检测系统的组成8.2.1事件产生器8.2.2事件分析器8.2.3事件数据库8.2.4事件响应单元8.3入侵检测系统的分类8.3.1按数据来源和系统结构分类8.3.2按工作原理分类8.3.3按时效性分类8.3.4按系统模块运行分布方式分类8.4.入侵检测系统的工作原理8.4.1入侵检测系统的检测流程8.4.2基于异常的入侵检测方法8.4.3基于误用的入侵检测方法8.5入侵检测系统的抗攻击技术8.5.1入侵响应8.5.2入侵跟踪技术8.5.3蜜罐技术8

<<网络安全基础教程与实训>>

.6入侵检测技术的发展方向8.6.1体系结构的新发展8.6.2应用层入侵检测8.6.3基于智能代理技术的分布式入侵检测系统8.6.4自适应入侵检测系统8.6.5提供高层统计与决策8.6.6响应策略与恢复研究8.6.7入侵检测的评测方法8.6.8与其他安全技术的结合8.7入侵检测工具与产品介绍8.7.1SessionWall-3 / eTrustIntrusionDetection8.7.2RealSecure8.7.3SkyBell8.7.4免费的IDS-Snort8.8本章实训实训：入侵检测软件SessionWall-3的安装与使用8.9本章习题第9章网络攻击与防范9.1网络攻防概述9.1.1网络攻击的一般目标9.1.2网络攻击的原理及手法9.1.3网络攻击的步骤及过程分析9.1.4网络攻击的防范策略9.2端口扫描9.2.1端口扫描的原理9.2.2端口扫描的常用工具及方法9.2.3端口扫描的防范对策9.3网络嗅探原理9.3.1嗅探器的概念9.3.2嗅探器攻击的检测9.3.3嗅探器的危害9.3.4网络嗅探的防范对策9.4密码攻防9.4.1密码攻防与探测破解原理9.4.2密码攻防与探测破解的常用工具及方法9.4.3密码攻防对策9.5特洛伊木马攻防9.5.1特洛伊木马攻击原理9.5.2特洛伊木马攻击的常用工具及方法9.5.3特洛伊木马程序的防范对策9.6缓冲区溢出攻防9.6.1缓冲区溢出的原理9.6.2缓冲区溢出攻击的防范方法9.6.3缓冲区溢出攻击示例9.7拒绝服务攻击与防范9.7.1拒绝服务攻防概述9.7.2拒绝服务模式分类9.7.3分布式拒绝服务攻击9.8本章实训实训：扫描器的使用实训2：破解密码实训3：木马攻击实训4：缓冲区溢出攻击实训5：拒绝服务攻击9.9本章习题第10章VPN技术10.1VPN的基本概念10.2VPN的系统特性10.2.1安全保障10.2.2服务质量保证10.2.3可扩充性和灵活性10.2.4可管理性10.2.5降低成本10.3VPN的原理与协议10.3.1实现VPN的隧道技术10.3.2PPTP协议10.3.3L2F协议10.3.4L2TP协议IO.3.5IPSec协议10.3.6SSLVPN10.3.7Windows2000的VPN技术10.4VPN典型应用需求10.4.1通过Internet实现远程用户访问10.4.2通过Internet实现网络互联10.4.3连接企业内部网络计算机10.5企业构建VPN的解决方案与相关设备10.5.1VPN硬件方案IO.5.2VPN软件方案10.5.3微软的VPN解决方案10.6本章实训实训1：WindOWS2000的数据链路层VPN配置实训2：Windows2000IPSecVPN协议配置实训3：windows2000SSL协议配置10.7本章习题参考文献

章节摘录

插图：

<<网络安全基础教程与实训>>

编辑推荐

针对性强，切合职业教育目标，重点培养职业能力，侧重技能传授实用性强，大量的经典真实案例，实训内容具体详细，与就业市场紧密结合适应性强，教程与实训二合一，适合于三年制和两年制高职高专，也同样适合于其他各类大中专院校强调知识的渐进、性、兼顾知识的系统性，结构逻辑性强，针对高职高专学生的知识结构特点安排教学内容书中配套形式多样的习题，网上提供完备的电子教案，提供相应的素材、程序代码、习题参考答案等教学资源，完全适合教学需要教材系列完整，涵盖计算机专业各个方向；编者分布广泛，结合不同地域特点，适合不同地域读者《网络安全基础教程与实训》着重从实践角度讲解计算机网络安全的基本概念、基本原理和技术方法。

各章配有习题，大部分章节配有相应的实训，便于教学和自学。

可作为高职高专院校计算机及相关专业的学生教材，也可作为计算机网络安全类的技术参考书或培训教材。

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>