第一图书网, tushu007.com

<<计算机网络技术及应用>>

图书基本信息

书名：<<计算机网络技术及应用>>

13位ISBN编号：9787512105324

10位ISBN编号：7512105320

出版时间：2011-4

出版时间：清华大学出版社

作者：杜柏林，罗秀波　主编

页数：437

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

第一图书网, tushu007.com

<<计算机网络技术及应用>>

内容概要

《计算机网络技术及应用》对计算机网络应用、数据通信、网络体系结构、局域网应用与组建、网络互连、网络管理、网络安全和windowsserver2003系统安装与服务器应用配置作了系统全面的介绍。

《计算机网络技术及应用》在结构安排上采取任务提出、任务知识和任务解决的方式，符合学习时认知规律，教学方法引人人胜。

《计算机网络技术及应用》内容丰富，图文并茂，基础理论知识讲解适度够用，动手实践内容具体详细，且很好地体现了理论与实践的结合，便于学生循序渐进地自学。

《计算机网络技术及应用》可作为大中专院校教材，亦可供从事入门网络知识学习及计算机网络管理人员的自学教材。

第一图书网, tushu007.com

<<计算机网络技术及应用>>

书籍目录

引入篇
第1章　网络发展概述及互联网络简单应用
知识1网络发展概述
知识2www服务及internet explorer浏览器应用
知识3电子邮件服务
知识4netmeeting服务
知识51p地址及子网划分
习题
基础篇
第2章　数据通信及网络组成体系
知识1数据通信系统
知识2网络体系结构
习题
第3章　局域网
知识1局域网的主要技术特征
知识2局域网组建及连接设备
知识3虚拟局域网(vlan)
知识4无线局域网
习题
第4章　网络互连
知识1网络互连概述
知识2路由器及路由配置
习题
第5章　windows server 2003的安装和配置
知识1网络操作系统概述
知识2windows server 2003操作系统安装和配置
习题
提高篇
第6章　广域网技术
知识1广域网及广域网常用技术
知识2广域网传输方法
习题
第7章　windows服务器应用配置
知识1iis服务器配置与管理
知识2dhcp服务器配置与管理
知识3dns服务器配置与管理
知识4邮箱服务器的配置与管理
习题
第8章　网络管理
知识1网络管理概述
知识2网络管理协议
知识3常见网络管理系统
习题
第9章　网络安全
知识1计算机网络不安全因素

第一图书网, tushu007.com

知识2网络“ 黑客 ”
知识3网络病毒
知识4网络防火墙技术
习题
第10章　互联网络的应用
知识1网上购物概述
知识2开通网上银行的步骤(以工商银行为例)
知识3网上银行的登录与密码修改
知识4网上银行的业务及密保卡的使用
知识5网上购物(淘宝网)
习题
第11章　网络布线
知识1综合布线系统知识
知识2布线器材与布线工具
习题
参考文献

第一图书网, tushu007.com

章节摘录

版权页：插图：（3）“ 黑客 ”入侵“ 黑客 ”的主要含义是非法入侵者。
“ 黑客 ”攻击网络的方法主要有：IP地址欺骗、发送邮件攻击、网络文件系统攻击、网络信息服务攻击、扫描器攻击、口令攻击、嗅探攻击、病毒和破坏性攻击等。
“ 黑客 ”通过寻找并利用网络系统的脆弱性和软件的漏洞，刺探窃取计算机口令、身份标识码或绕过计算机安全控制机制，非法进入计算机网络或数据库系统，窃取信息。
现在全球每20秒钟就有一起“ 黑客 ”事件发生。
按“ 黑客 ”的动机和造成的危害，目前“ 黑客 ”分为恶作剧、盗窃诈骗、蓄意破坏、控制占有、窃取情报等类型。
其中，西方一些国家的情报部门秘密招聘“ 黑客 ”“ 高手 ”，编制专门的“ 黑客 ”程序，用于窃取别国（集团）因特网或内部网上的涉密信息和敏感信息。
（4）软件隐患许多软件在设计时，为了方便用户的使用、开发和资源共享，总是留有许多“ 窗口 ”，加上在设计时不可避免地存在许多不完善或未发现的漏洞，用户在使用过程中，如果缺乏必要的安全鉴别和防护措施，.就会使攻击者利用上述漏洞侵入信息系统破坏和窃取信息。
目前，不少单位使用的软件是国外产品，这给信息安全保密带来很大困难。
（5）设备隐患主要指计算机信息系统中硬件设备存在的漏洞和缺陷。
①电磁泄漏发射。
电磁泄漏发射是指信息系统的设备在工作时向外辐射电磁波的现象。
计算机的电磁辐射主要有两种途径：一是被处理的信息会通过计算机内部产生的电磁波向空中发射，称为辐射发射；二是这种含有信息的电磁波也可以经电源线、信号线、地线等异体传送和辐射出去，称为传导发射。
这些电磁辐射包含数据信息和视频信息等内容。
这些辐射出去的电磁波，任何人都可借助仪器设备在一定范围内收到它，尤其是利用高灵敏度的仪器可稳定清晰地获取计算机正在处理的信息。
日本的一项试验结果表明：未加屏蔽的计算机启动后，用普通计算机可以在80米内接收其显示器上的内容。
据报道，国际高灵敏度专用接收设备可在1公里外接收并还原计算机的辐射信息。
早在20世纪80年代，国外情报部门就把通过接收计算机电磁辐射信息作为窃密的重要手段之一。
②磁介质的剩磁效应。
存储介质中的信息被删除后，有时仍会留下可读痕迹；即使已多次格式化的磁介质（盘、带）仍会有剩磁，这些残留信息可通过“ 超导量子干涉器件 ”还原出来。
在大多数的操作系统中，删除文件只是删除文件名，而原文件还原封不动地保留在存储介质中，从而留下泄密隐患。
③预置陷阱。
即人为地在计算机信息系统中预设一些陷阱，干扰和破坏计算机信息系统的正常运行。
预置的陷阱一般分为硬件陷阱和软件陷阱两种。
其中，硬件陷阱主要是“ 芯片捣鬼 ”，即蓄意更改集成电路芯片的内容设计和使用规程，以达到破坏计算机信息系统的目的。
计算机信息系统中一个关键芯片的小小故障，就足以导致计算机甚至整个信息网络停止运行。

第一图书网, tushu007.com

编辑推荐

第一图书网, tushu007.com

<<计算机网络技术及应用>>

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