

<<计算机网络安全>>

图书基本信息

书名：<<计算机网络安全>>

13位ISBN编号：9787111335054

10位ISBN编号：7111335058

出版时间：2011-4

出版时间：鲁立、龚涛 机械工业出版社 (2011-04出版)

作者：鲁立，龚涛 编

页数：242

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>

<<计算机网络安全>>

内容概要

《计算机网络安全》围绕网络安全应用技术，由浅入深、循序渐进地介绍了计算机网络安全方面的知识，同时注重对学生的实际应用技能和动手能力的培养。

全书共分9章，内容涵盖网络基础知识、计算机病毒、加密与数字签名技术、操作系统漏洞、防火墙技术、端口扫描技术、入侵检测以及无线局域网安全。

本书内容丰富翔实，通俗易懂，以实例为中心，并结合大量的经验技巧。

《计算机网络安全》既可作为各大高职高专院校计算机以及相关专业的教材，也可作为网络安全管理员指导用书。

<<计算机网络安全>>

书籍目录

出版说明前言第1章 计算机网络安全概述1.1 计算机网络安全的基本概念1.1.1 网络安全的定义1.1.2 网络安全的特性1.2 计算机网络安全的威胁1.2.1 网络安全威胁的分类1.2.2 计算机病毒的威胁1.2.3 木马程序的威胁1.2.4 网络监听1.2.5 黑客攻击1.2.6 恶意程序攻击1.3 网络安全威胁产生的根源1.3.1 系统及程序漏洞1.3.2 网络安全防护所需设施存在的问题1.3.3 安全防护知识方面存在的问题1.4 网络安全策略1.4.1 网络安全策略设计的原则1.4.2 几种网络安全策略1.5 计算机网络安全的现状与发展1.5.1 计算机网络安全的现状1.5.2 计算机网络安全的发展方向1.6 小结与练习1.6.1 小结1.6.2 练习第2章 网络安全体系结构及协议2.1 计算机网络协议概述2.1.1 网络协议2.1.2 协议簇和行业标准2.1.3 协议的交互2.1.4 技术无关协议2.2 OSI参考模型及其安全体系2.2.1 计算机网络体系结构2.2.2 OSI参考模型简介2.2.3 ISO/OSI安全体系2.3 TCP/IP参考模型及其安全体系2.3.1 TCP/IP参考模型2.3.2 TCP/IP参考模型的安全体系2.4 常用网络协议和服务2.4.1 常用网络协议2.4.2 常用网络服务2.5 Windows常用的网络命令2.5.1 ping命令2.5.2 at命令2.5.3 netstat命令2.5.4 tracert命令2.5.5 net命令2.5.6 ftp命令2.5.7 nbtstat命令2.5.8 telnet命令2.6 协议分析工具-Sniffer的应用2.6.1 Sniffer的启动和设置2.6.2 解码分析2.7 实训项目2.8 小结与练习2.8.1 小结2.8.2 练习第3章 计算机病毒与木马3.1 计算机病毒概述3.1.1 计算机病毒的定义3.1.2 计算机病毒的演变史3.1.3 计算机病毒的特性3.2 计算机病毒及其分类、传播途径3.2.1 常见计算机病毒3.2.2 计算机病毒的分类3.2.3 计算机病毒的传播途径3.3 计算机病毒的检测和防御3.3.1 普通计算机病毒的检测与防御3.3.2 U盘病毒的检测与防御3.3.3 ARP病毒的检测与防御3.3.4 蠕虫病毒的检测与防御3.4 计算机木马概述3.4.1 计算机木马的定义3.4.2 计算机木马的类型及基本功能3.4.3 计算机木马的工作原理3.5 计算机木马的检测与防御3.5.1 普通计算机木马的检测与防御3.5.2 典型计算机木马的手动清除3.6 实训项目3.7 小结与练习3.7.1 小结3.7.2 练习第4章 加密与数字签名4.1 加密技术4.1.1 加密技术概述4.1.2 数据加密常见方式4.2 加密算法4.2.1 古典加密算法4.2.2 现代加密算法4.3 数字签名技术4.3.1 数字签名技术概述4.3.2 数字签名技术的工作原理4.3.3 数字签名技术的算法4.4 PKI技术4.4.1 PKI概述4.4.2 PKI技术原理4.4.3 证书颁发机构4.4.4 数字证书4.5 PGP原理及应用4.5.1 PGP概述4.5.2 PGP密钥的创建4.5.3 PGP文件加密和解密4.5.4 PGP密钥导出与导入4.5.5 PGP电子邮件加、解密和签名验证4.5.6 PGP数字签名4.6 EFS原理及应用4.6.1 EFS概述4.6.2 EFS的加密和解密4.6.3 EFS的其他应用4.7 SSL安全传输及应用4.7.1 SSL概述4.7.2 SSL的工作原理4.7.3 安装证书服务4.7.4 申请证书4.7.5 颁发Web服务器证书4.7.6 安装服务器证书4.7.7 Web服务器的SSL设置4.7.8 浏览器的SSL设置4.7.9 访问SSL站点4.8 实训项目4.9 小结与练习4.9.1 小结4.9.2 练习第5章 防火墙技术5.1 防火墙概述5.1.1 防火墙的基本准则5.1.2 防火墙的主要功能特性5.1.3 防火墙的局限性5.2 防火墙的实现技术5.2.1 数据包过滤5.2.2 应用层代理5.2.3 状态检测技术5.3 防火墙的体系结构5.3.1 双宿/多宿主主机模式5.3.2 屏蔽主机模式5.3.3 屏蔽子网模式5.4 防火墙的工作模式5.5 防火墙的实施方式5.5.1 基于单个主机的防火墙5.5.2 基于网络主机的防火墙5.5.3 硬件防火墙5.6 瑞星个人防火墙的应用5.6.1 界面与功能布局5.6.2 常用功能5.6.3 网络监控5.6.4 访问控制5.6.5 高级设置5.7 ISA Server 2004配置5.7.1 ISA Server 2004概述5.7.2 ISA Server 2004的安装5.7.3 ISA Server 2004防火墙策略5.7.4 发布内部网络中的服务器5.7.5 ISA Server 2004的系统和网络监控及报告5.8 iptables防火墙5.8.1 iptables中的规则表5.8.2 iptables命令简介5.8.3 Linux防火墙配置5.9 PIX防火墙配置5.9.1 PIX的基本配置命令5.9.2 PIX防火墙配置实例5.10 实训项目5.11 小结与练习5.11.1 小结5.11.2 练习第6章 Windows Server 2003的网络安全6.1 Windows Server 2003的安全简介6.1.1 用户身份验证6.1.2 基于对象的访问控制6.2 Windows Server 2003系统安全配置的常用方法6.2.1 安装过程6.2.2 正确设置和管理账户6.2.3 正确设置目录和文件权限6.2.4 网络服务安全管理6.2.5 关闭无用端口6.2.6 本地安全策略6.2.7 审核策略6.2.8 Windows日志文件的保护6.3 Windows Server 2003访问控制技术6.3.1 访问控制技术简介6.3.2 Windows Server 2003访问控制的使用6.4 账户策略6.4.1 账户策略的配置6.4.2 Kerberos策略6.5 启用安全模板6.5.1 安全模板的简介6.5.2 启用安全模板的方法6.6 实训项目6.7 小结与练习6.7.1 小结6.7.2 练习第7章 端口扫描技术7.1 端口概述7.1.1 TCP/IP工作原理7.1.2 端口的定义7.1.3 端口的分类7.2 端口扫描技术7.2.1 端口扫描概述7.2.2 常见的端口扫描技术7.3 常见扫描软件及其应用7.3.1 扫描软件概述7.3.2 Super Scan扫描工具及应用7.4 端口扫描防御技术应用7.4.1 查看端口的状态7.4.2 关闭闲置和危险的端口7.4.3 隐藏操作系统类型7.5 实训项目7.6 小结与练习7.6.1 小结7.6.2 练习第8章 入侵检测系统8.1 入侵检测概述8.1.1 入侵检测的概念及功能8.1.2 入侵检测系统模型8.1.3 入侵检测

<<计算机网络安全>>

工作过程8.2 入侵检测系统的分类8.2.1 根据检测对象划分8.2.2 根据检测技术划分8.2.3 根据工作方式划分8.3 入侵检测系统部署8.3.1 基于主机的入侵检测系统部署8.3.2 基于网络的入侵检测系统部署8.3.3 常见入侵检测工具及其应用8.4 入侵防护系统8.4.1 入侵防护系统的工作原理8.4.2 入侵防护系统的优点8.4.3 入侵防护系统的主要应用8.5 小结与练习8.5.1 小结8.5.2 练习第9章 无线网络安全9.1 无线局域网介绍9.1.1 无线局域网常用术语9.1.2 无线局域网组件9.1.3 无线局域网的访问模式9.1.4 覆盖区域9.2 无线网络常用标准9.2.1 IEEE802.11b9.2.2 IEEE802.11a9.2.3 IEEE802.11g9.2.4 IEEE802.11n9.3 无线网络安全解决方案9.3.1 无线网络访问原理9.3.2 认证9.3.3 加密9.3.4 入侵检测系统9.4 小结与练习9.4.1 小结9.4.2 练习参考文献

<<计算机网络安全>>

章节摘录

版权页：插图：（2）系统信息安全对系统信息安全而言，网络安全主要指保证在信息处理和传输系统中存储和传输的信息安全（即保证网络数据的完整性、可用性和机密性），如信息不被非法访问、散布、窃取、篡改、删除、识别和使用等。

1.1.2 网络安全的特性在美国国家信息基础设施的文献中，提出了网络安全的5个特性：可用性、机密性、完整性、可靠性和不可抵赖性。

这5个特性适用于国家信息设施的各个领域。

（1）可用性得到授权的用户在需要时可访问数据，也就是说，攻击者不能占用资源而妨碍授权用户正常使用资源。

授权的用户随时可以访问到需要使用的信息，这里的主要目的是确保硬件可以使用，信息能够被访问

。黑客攻击可以导致系统资源被耗尽，这就是对可用性做的攻击。

对用户而言，网络是支持工作的载体，网络资源和网络服务发生中断，可能带来巨大的经济和社会影响，因此网络安全体系必须保证网络资源和服务的连续、正常的运行，要防止破坏网络的可用性。

（2）机密性确保信息不泄露给非授权用户、实体或进程；用于保障网络机密性的技术主要是密码技术；在网络的不同层次上有不同的机制来保障机密性。

通过授权可以控制用户是否可以访问以及访问的程度。

（3）完整性完整性是指信息在处理过程中不受到破坏、不会被修改。

只有得到允许的用户才能修改数据，并可以判断数据是否被修改。

即信息在存储或传输过程中保持不被修改、不被破坏和不丢失的特性。

（4）可靠性可靠性是指系统在规定的条件下和规定的时间内，完成规定功能的概率。

可靠性是网络安全最基本的要求之一。

<<计算机网络安全>>

编辑推荐

《计算机网络安全》：全国高等职业教育规划教材。

<<计算机网络安全>>

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>