<<计算机安全技术>>

图书基本信息

书名：<<计算机安全技术>>

13位ISBN编号：9787302235651

10位ISBN编号：7302235651

出版时间：2010-9

出版时间：清华大学出版社

作者：张同光 编

页数：365

前言

随着计算机的普及以及互联网的建设向纵深发展（比如物联网的迅速发展），计算机技术和网络技术已深入到社会的各个领域，人类对计算机和计算机网络的依赖越来越大，计算机安全问题已经成为全社会关注和讨论的焦点。
如何保护企业或个人的计算机系统免遭非法入侵，如何防止计算机病毒、木马等对内部网络的侵害，都是信息时代企业或个人面临的实际问题。
因此，社会对计算机安全技术的需求也越来越迫切。
为了满足社会的需要，各高等院校计算机相关专业相继开设了计算机安全方面的课程。
但是，目前多数计算机安全技术方面的教材偏重于理论，不能很好地激发学生学习这门课的兴趣，所以，为了满足计算机安全技术教学方面的需求，笔者编写了本书。
本书以解决具体计算机安全问题为目的，全面介绍计算机安全领域的实用技术，帮助读者了解计算机安全技术体系，掌握维护计算机系统安全的常用技术和手段，解决实际计算机系统的安全问题，使读者从全方位建立起对计算机安全保障体系的认识。
本书共8章。
第1章介绍计算机安全的基本概念、计算机安全面临的威胁以及计算机安全技术体系结构。
通过本章的学习，使读者对计算机安全有一个整体的认识。
第2章通过对环境安全、设备安全、电源系统安全以及通信线路安全的详细介绍，帮助读者了解物理安全的相关知识，并且能够运用本章介绍的知识和技术来保障计算机系统的物理安全。
第3章介绍常用加密方法、密码学的基本概念、破解用户密码的方法、文件加密的方法、数字签名技术以及PKI，并且通过对一系列实例的介绍，加深读者对基础安全方面的基础知识和技术的理解，使读者能够运用一些工具软件来保护自己在工作或生活中的机密或隐私数据。
第4章主要介绍Windows系统中账号安全管理、网络安全管理、IE浏览器的安全设置、组策略的使用、Windows权限的概念及其设置、Windows安全审计，然后简单介绍UNIX／Linux系统安全的配置，通过本章的学习，使读者了解Windows系统安全的多个方面，从而提高读者安全使用Windows系统的水平。
第5章介绍端口与漏洞扫描以及网络监听技术、缓冲区溢出攻击及其防范、ARP欺骗、DoS与DDoS攻击检测与防御、防火墙技术、入侵检测与入侵防御技术、恶意软件、蜜罐技术、VPN技术、HTTPTunneel技术以及无线网络安全等内容，并且通过对一系列实例的介绍，加深读者对网络安全和攻防方面的基础知识和技术的理解，帮助读者提高解决实际网络安全问题的能力。

<<计算机安全技术>>

内容概要

本书本着“理论够用，重在实践”的原则，采用案例引导理论阐述的编写方法，内容注重实用，结构清晰，图文并茂，通俗易懂，力求做到让读者在兴趣中学习计算机安全技术。

本书共8章，主要内容包括：计算机安全概述、实体和基础设施安全、密码技术、操作系统安全技术、计算机网络安全技术、数据库系统安全技术、应用安全技术、容灾与数据备份技术。

本书适合作为高职高专及成人高等院校电子信息类专业教材，也可供培养技能型紧缺人才的相关院校及培训班教学使用。

<<计算机安全技术>>

书籍目录

第1章 计算机安全概述 1.1 计算机安全基本概念 1.2 计算机安全研究的重要性 1.3 计算机安全技术体系结构 1.3.1 实体和基础设施安全技术 1.3.2 密码技术 1.3.3 操作系统安全技术 1.3.4 计算机网络安全技术 1.3.5 应用安全技术 1.4 计算机安全发展趋势 1.5 安全系统设计原则 1.6 人、制度和技术之间的关系 小结 习题第2章 实体和基础设施安全 2.1 物理安全的重要性 2.2 计算机机房及环境安全 2.3 设备安全 2.4 供电系统安全 2.5 通信线路安全与电磁辐射防护 小结 习题第3章 密码技术 3.1 密码技术基础 3.2 常用加密方法 3.2.1 实例：使用压缩工具加密 3.2.2 实例：Office文件加密与解密 3.2.3 实例：使用加密软件PGP 3.3 用户密码的破解 3.3.1 实例：破解windows用户密码 3.3.2 实例：破解Linux用户密码 3.3.3 密码破解工具John the Ripper 3.3.4 用户密码的保护 3.4 文件加密 3.4.1 实例：用对称加密算法加密文件 3.4.2 对称加密算法 3.4.3 实例：用非对称加密算法加密文件 3.4.4 非对称加密算法 3.4.5 混合加密体制算法 3.5 数字签名 3.5.1 数字签名概述 3.5.2 实例：数字签名 3.6 PKI技术 3.7 实例：构建基于Windows 2003的CA系统 小结 习题第4章 操作系统安全技术 4.1 操作系统安全基础 4.2 windows安全体系结构 4.3 实例：windows系统安全配置 4.3.1 账号安全管理 4.3.2 网络安全管理 4.3.3 IE浏览器 4.3.4 注册表 4.3.5 Windows组策略 4.3.6 Windows权限 4.3.7 Windows安全审计 4.4 Linux自主访问控制与强制访问控制 4.5 实例：Linux系统安全配置 4.5.1 账号安全管理 4.5.2 存取访问控制 4.5.3 资源安全管理 4.5.4 网络安全管理 4.6 安全等级标准 4.6.1 ISO安全体系结构标准 4.6.2 美国可信计算机安全评价标准 4.6.3 中国国家标准《计算机信息系统安全保护等级划分准则》 小结 习题第5章 计算机网络安全技术 5.1 计算机网络安全概述 5.1.1 网络安全面临的威胁 5.1.2 网络安全的目标 5.1.3 网络安全的特点 5.2 黑客攻击简介 5.2.1 黑客攻击的目的和手段 5.2.2 黑客攻击的步骤 5.2.3 黑客入门 5.2.4 黑客攻击常用工具及常见攻击形式 5.3 实例：端口与漏洞扫描及网络监听 5.4 缓冲区溢出 5.4.1 实例：缓冲区溢出及其原理 5.4.2 实例：缓冲区溢出攻击及其防范 5.5 ARP欺骗 5.5.1 实例：ARP欺骗 5.5.2 ARP欺骗的原理与防范 5.6 DOS与DDoS攻击检测与防御 5.6.1 实例：DDoS攻击 5.6.2 DOS与DDoS攻击的原理 5.6.3 DOS与DDoS攻击检测与防范 5.7 防火墙技术 5.7.1 防火墙的功能与分类 5.7.2 实例：Windows中防火墙的配置 5.7.3 实例：Linux防火墙配置 5.8 入侵检测技术 5.8.1 实例：使用Snort进行入侵检测 5.8.2 入侵检测技术概述 5.9 入侵防御技术 5.9.1 入侵防御技术概述 5.9.2 实例：入侵防御系统的搭建 5.10 恶意软件 5.10.1 计算机传统病毒的基本概念 5.10.2 蠕虫病毒 5.10.3 特洛伊木马 5.10.4 实例：宏病毒的创建与清除 5.10.5 实例：反向连接木马的传播 5.10.6 实例：网页病毒、网页挂马 5.10.7 网页病毒、网页挂马的基本概念 5.10.8 实例：查看开放端口判断木马 5.10.9 方法汇总——病毒、蠕虫、木马的清除和预防 5.10.10 流行杀毒软件简介 5.11 实例：蜜罐技术 5.12 VPN技术 5.12.1 VPN技术概述 5.12.2 实例：配置基于Windows平台的VPN 5.12.3 实例：配置基于Linux平台的VPN 5.13 实例：httptunnel技术 5.14 实例：无线网络安全配置 小结 习题第6章 数据库系统安全技术 6.1 SQL注入式攻击 6.1.1 实例：注入攻击MS SQL Server 6.1.2 实例：注入攻击Access 6.1.3 SQL注入式攻击的原理及技术汇总 6.1.4 如何防范SQL注入攻击 6.2 常见的数据库安全问题及安全威胁 6.3 数据库系统安全体系、机制和需求 6.3.1 数据库系统安全体系 6.3.2 数据库系统安全机制 6.3.3 数据库系统安全需求 6.4 数据库系统安全管理 6.4.1 实例：MS SQL Server 2005安全管理 6.4.2 数据库安全管理原则 6.5 数据库的备份与恢复 小结 习题第7章 应用安全技术 7.1 Web应用安全技术 7.1.1 Web技术简介与安全分析 7.1.2 应用安全基础 7.1.3 实例：XSS跨站攻击技术 7.2 电子商务安全 7.3 实例：电子邮件加密 7.4 实例：垃圾邮件的处理 7.5 实例：网络防钓鱼技术 7.6 实例：QQ安全使用 7.7 网上银行账户安全 7.8 实例：使用WinHex 小结 习题第8章 容灾与数据备份技术 8.1 容灾技术 8.1.1 容灾技术概述 8.1.2 RAID简介 8.1.3 数据恢复工具 8.2 数据备份技术 8.3 Ghost 8.3.1 Ghost概述 8.3.2 实例：用Ghost备份分区(系统) 8.3.3 实例：用Ghost恢复系统 小结 习题附录 网络服务、木马与端口对照表参考文献

章节摘录

插图：密码学是研究编制密码和破译密码的技术科学。
研究密码变化的客观规律，应用于编制密码以保守通信秘密的，称为编码学；应用于破译密码以获取通信情报的，称为破译学，总称密码学。
密码学是在编码与破译的斗争实践中逐步发展起来的，并随着先进科学技术的应用，已成为一门综合性的尖端技术科学。
它与语言学、数学、电子学、声学、信息论、计算机科学等有着广泛而密切的联系。
它的现实研究成果，特别是各国政府现用的密码编制及破译手段都具有高度的机密性。
利用文字和密码的规律，在一定条件下，采取各种技术手段，通过对截取密文的分析，以求得明文，还原密码编制，即破译密码。
破译不同强度的密码，对条件的要求也不相同，甚至完全不同。
密码破译是随着密码的使用而逐步产生和发展的。
1412年，波斯人卡勒卡尚迪所编的百科全书中载有破译简单代替密码的方法。
到16世纪末期，欧洲一些国家设有专职的破译人员，以破译截获的密信。
密码破译技术有了相当大的发展。
1863年普鲁士人卡西斯基所著《密码和破译技术》以及1883年法国人克尔克霍夫所著《军事密码学》等著作，都对密码学的理论和方法做过一些论述和探讨。
1949年美国人香农发表了《秘密体制的通信理论》一文，应用信息论的原理分析了密码学中的一些基本问题。
1917年，英国破译了德国外长齐默尔曼的电报，促成了美国对德宣战。
1942年，美国从破译日本海军密报中，获悉日军对中途岛地区的作战意图和兵力部署，从而以劣势兵力击破日本海军的主力，扭转了太平洋地区的战局。
这些事例也从反面说明了密码保密的重要性。
如今许多国家都十分重视密码工作，设立相关机构，拨出巨额经费，集中专家和科技人员，投入大量高速的电子计算机和其他先进设备进行工作。
各民间企业和学术界也对密码日益重视，不少数学家、计算机学家和其他有关学科的专家也投身于密码学的研究行列，更加速了密码学的发展。
总之，计算机安全主要包括系统安全和数据安全两个方面。
而数据安全则主要采用现代密码技术对数据进行安全保护，如数据保密、数据完整性、身份认证等技术。
密码技术包括密码算法设计、密码分析、安全协议、身份认证、消息确认、数字签名、密钥管理、密钥托管等技术，是保护大型网络安全传输信息的唯一有效手段，是保障信息安全的核心技术。
密码技术以很小的代价，对信息提供一种强有力的安全保护。

<<计算机安全技术>>

编辑推荐

《计算机安全技术》：21世纪高职高专规划教材·计算机应用系列

<<计算机安全技术>>

版权说明