

《计算机网络安全原理与实现》

图书基本信息

书名：《计算机网络安全原理与实现》

13位ISBN编号：9787111245315

10位ISBN编号：7111245318

出版时间：2009-1

出版社：刘海燕 机械工业出版社 (2009-01出版)

页数：286

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu000.com

前言

随着信息化的发展，网络已经渗透到社会的各个领域，对科学、技术、政治、经济、军事乃至人类的生活都产生了巨大的影响。网络已经成为人类社会的一项关键基础设施，发挥着至关重要的作用。然而，由于网络规模的不断扩大，网络复杂性随之增强，网络安全问题日益凸显，已经成为阻碍网络应用普及的一个关键要素。《计算机网络安全原理与实现》围绕“网络攻击和防护技术”这一核心问题展开，重点介绍网络攻击和防护技术的原理，并通过简单示例分析技术的实现。全书分为网络安全基础、网络安全中的攻击技术、网络安全中的防护技术三个部分。第一篇包括第1~3章，目的是补充读者在网络协议、网络攻防编程方面的基础知识。第1章回顾网络协议的内容，重点强调协议中与攻击和防护有关的部分。UNIX / Linux和Windows是计算机使用的两类主流平台。第2章介绍uNix / Linux平台上的网络程序设计基础知识，包括编写TCP / IP程序、原始套接字的使用、使用libpcap捕获数据包、使用libnet构造数据包等知识。第3章介绍Windows平台上的攻防编程，分别介绍Windows下的TCP / UDP编程、原始套接字的使用以及如何操作注册表。第二篇包括第4~6章，内容涵盖网络攻击的概念、原理和方法。第4章概述网络攻击的发展历史、概念、目标和分类，介绍攻击的基本步骤以及发展趋势。第5章介绍常用的几种攻击技术。对每种技术，按照先介绍相关的概念和原理，接着分析其实现技术并给出演示性的示例，最后介绍如何进行防范的顺序组织内容。通过该章的学习，可以加深对网络攻击技术的理解，掌握相关的防范措施。第6章介绍恶意软件技术，包括病毒技术、蠕虫技术和木马技术，对于每种技术都说明其一般性原理，并给出一些简单的示例。通过这些示例，读者可以加深对恶意软件工作原理的理解，提高防范能力。第三篇包括第7~12章，内容涉及防护的总体概念以及一些常用的防护技术。第7章介绍安全体系和安全模型的概念以及有关的安全评估标准。第8章介绍密码学，包括对称密钥密码算法、非对称密钥密码算法以及单向散列函数，还将介绍PGP软件的安装和使用，第9章介绍身份认证的概念和主要的认证技术，第10章介绍访问控制策略及其实现机制；第11章介绍防火墙的有关概念和实现技术；第12章介绍入侵检测的原理和实现技术。对每种技术，力求讲清其工作原理，介绍常用工具的使用方法并给出实现示例。《计算机网络安全原理与实现》既是作者多年来从事教学一线工作经验的总结，也是近年来信息安全技术和网络对抗技术发展的最新成果的体现。由于作者水平有限、时间仓促，加之网络攻防技术发展迅猛，新的知识、原理和技术层出不穷，书中难免存在一些缺点和错误，恳请广大读者不吝赐教，批评指正。

《计算机网络安全原理与实现》

内容概要

《计算机网络安全原理与实现》系统阐述计算机网络安全的基本原理、技术和方法，包括网络安全基础、网络安全中的攻击技术以及网络安全中的防护技术三大部分。第一篇主要介绍网络协议以及网络攻防编程的基础知识；第二篇主要介绍网络攻击的概念、目标和分类以及攻击的原理及防范方法，并介绍恶意软件技术；第三篇主要介绍网络安全体系结构以及加密技术、认证技术、访问控制、防火墙技术、入侵检测技术等。

《计算机网络安全原理与实现》取材新颖，概念清晰，既可以作为高等院校相关专业本科生、研究生的教学用书，也是网络安全防护人员、网络安全产品开发人员和网络对抗研究人员的参考资料。

作者简介

刘海燕，女，汉族，1963年8月出生。1998年晋升为北京理工大学副教授，现为北京理工大学工程力学骨干讲员。参加工作以来一直工作在基础教学的第一线，曾先后主讲了《理论力学》（多、中、少学时），《机械振动》，《计算机导论》，《计算机应用基础》，《工程力学A》，《工程力学C》等本科生课程。1996年获校青年教师优秀教学成果三等奖。1997年获校三育人优秀教师称号，同年被评为校优秀青年骨干教师，并获得SMC奖学金二等奖。1998年获校青年教师教学基本功比赛鼓励奖。1999年“工程力学课程教学体系和内容改革”获第九届校优秀教学成果一等奖（集体成员之一）；2003年“工程力学课程立体化教学改革与实践”获校第十一届优秀教学成果一等奖（集体成员之一）；2004年“工程力学课程教学改革与实践”获北京市高等教育教学成果一等奖（集体成员之一），2005年获高等教育国家级教学成果二等奖（集体成员之一）。《工程力学》（上、下册），2003年高等教育出版社出版，本人编写该教材中原理论力学的部分内容，所写字数达20万字，该教材为普通高等教育“十五”国家级规划教材及北京市高等教育精品教材。《工程力学学习指导》（上、下册），本人编写与主教材配套的相关部分，2003年8月由北京理工大学出版社出版。

第一篇 网络安全基础	第1章 网络协议安全基础	1.1 计算机网络的体系结构	1.1.1 OSI参考模型	1.1.2 TCP / IP体系结构	1.2 TCP / IP协议族	1.2.1 链路层协议	1.2.2 网络层协议	1.2.3 传输层协议	1.2.4 常用的应用层协议	13																														
	本章 小结习题	第2章 UNIX / Linux下的网络程序设计	2.1 套接字编程基础	2.2 基于TCP协议的网络编程	2.2.1 创建套接字函数socket	2.2.2 绑定函数bind	2.2.3 监听函数listen	2.2.4 接受函数accept	2.2.5 连接函数connect	2.2.6 连接中止函数close	2.2.7 连接关闭函数shutdown	2.2.8 写函数write	2.2.9 读函数read	2.2.10 基于TCP协议的网络程序结构	2.2. TCP网络程序示例	2.3 基于JDP协议的网络编程	2.3.1 常用的收发函数	2.3.2 基于13DP协议的网络程序结构	2.3.3 LJDIP网络程序示例	2.4 其他常用函数	2.4.1 IP地址和域名的转换函数	2.4.2 服务信息函数	2.4.3 其他读写函数	2.5 原始套接字	2.5.1 原始套接字的创建	2.5.2 原始套接字的发送	2.5.3 原始套接字的接收	2.5.4 常用协议首部结构定义	2.5.5 原始套接字编程示例	2.6 网络数据包捕获开发包libpcap	2.6.1 libpcap的安装	2.6.2 libpcap库用程序框架	2.6.3 libpcap包捕获机制分析	2.6.4 libpcap数据包过滤机制	2.6.5 libpcap编程示例	2.7 网络数据包构造函数库libnet	2.7.1 libnet简介	2.7.2 libnet的函数	2.7.3 libnet编程示例	2.8 本章 小结习题
	第3章 Windows攻防编程	3.1 WindowsSocket网络编程	3.1.1 WinSock的初始化	3.1.2 建立Socket	3.1.3 基于rcP协议的网络编程	3.1.4 UDP协议编程	3.2.原始套接字	3.2.1 创建一个原始套接字	3.2.2 构造数据包	3.2.3 发送原始套接字数据包	3.2.4 使用原始套接字接收数据	3.2.5 原始套接字编程示例	3.3 注册表编程	3.3.1 注册表操作函数	3.3.2 注册表操作程序示例	3.4 本章 小结习题																								
	第二篇 网络安全中的攻击技术	第4章 网络攻击的概念与发展	4.1 网络攻击与信息安全	4.2 网络攻击的目标和分类	4.2.1 网络攻击目标	4.2.2 网络攻击的分类方法	4.3 网络攻击的基本过程	4.4 网络攻击技术的演变	4.5 本章 小结习题																															
	第5章 网络攻击技术原理	5.1 网络欺骗	5.1.1 IP欺骗	5.1.2 电子邮件欺骗	5.1.3 Web欺骗	5.1.4 非技术类欺骗	5.1.5 网络欺骗的防范	5.2 嗅探技术	5.2.1 以太网嗅探原理	5.2.2 嗅探器的实现	5.2.3 嗅探器的检测与防范	5.3 扫描技术	5.3.1 网络扫描诊断命令	5.3.2 端口扫描	5.3.3 操作系统探测	5.3.4 脆弱性扫描	5.3.5 扫描的防范	5.4 口令破解技术	5.4.1 Linux离线口令破解实例	5.4.2 WindowsNT / 2000的口令机制	5.4.3 口令窃听	5.4.4 口令破解的防范	5.5 缓冲区溢出攻击	5.5.1 什么是缓冲区溢出	5.5.2 缓冲区溢出的原理	5.5.3 缓冲区溢出漏洞的普遍性	5.5.4 缓冲区溢出攻击示例	5.5.5 缓冲区溢出攻击的类型	5.6 拒绝服务攻击	5.6.1 Smurf攻击	5.6.2 SYN洪泛攻击	5.6.3 Teardrop攻击	5.6.4 DDoS攻击	5.7 本章 小结习题						
	第6章 恶意软件技术原理	6.1 恶意软件的演变	6.2 什么是恶意软件	6.3 恶意软件的特征	6.4 什么不是恶意软件	6.5 病毒	6.5.1 病毒的定义	6.5.2 病毒的结构	6.5.3 病毒的分类	6.5.4 宏病毒	6.5.5 脚本病毒	6.5.6 计算机病毒的防治技术	6.6 蠕虫	6.6.1 蠕虫概述	6.6.2 典型蠕虫分析	6.6.3 蠕虫编写示例	6.7 木马	6.7.1 木马的原理	6.7.2 木马技术的发展	6.7.3 木马编写示例	6.7.4 木马的发现与清除方法	6.7.5 木马的高级技术	6.8 本章 小结习题																	
	第三篇 网络安全中的防护技术	第7章 安全体系结构与安全模型	7.1 安全体系结构	7.1.1 什么是安全体系结构	7.1.2 开放式系统互连安全体系结构	7.1.3 TCP / IP协议的安全体系结构	7.2 安全模型	7.2.1 多级安全模型	7.2.2 多边安全模型	7.2.3 p2DR安全模型	7.3 安全评估标准	7.3.1 TCSEC标准	7.3.2 CC标准	7.3.3 我国的计算机安全等级划分与相关标准	7.4 本章 小结习题																									
	第8章 密码学	8.1 密码学概述	8.1.1 密码学的历史	8.1.2 密码学的基本概念	8.1.3 密码算法的分类	8.1.4 网络通信中的加密方式	8.1.5 密码的破译	8.1.6 密码算法的安全性	8.2 简单密码算法	8.2.1 替换密码	8.2.2 易位密码	8.2.3 一次一密	8.3 对称密钥密码算法	8.3.1 pEs对称密钥密码算法	8.3.2 三重DES	8.3.3 IDEA加密算法简介	8.3.4 加密模式	8.4 公开密钥密码算法	8.4.1 公开密钥密码算法原理	8.4.2 RSA算法简介	8.4.3 RSA算法的安全性	8.5 单向散列函数	8.5.1 单向散列函数的原理	8.5.2 MD5算法	8.5.3 其他散列算法	8.6 消息认证	8.6.1 消息认证码	8.6.2 消息认证码的实现	8.6.3 消息认证的安全性分析	8.7 数字签名	8.7.1 数字签名的原理	8.7.2 数字签名的实现方式	8.8 PGP软件	8.8.1 PGP软件简介	8.8.2 PGP软件的安装	8.8.3 PGP软件的使用	8.9 本章 小结			
	第9章 身份认证技术	9.1 身份认证技术概述	9.1.1 身份认证的基本概念	9.1.2 身份认证的形式	9.2 基于口令的身份认证	9.2.1 简单口令认证	9.2.2 质询 / 响应认证	9.2.3 一次性口令	9.2.4 双因素认证	9.2.5 RADILJS协议	9.2.6 口令的管理	9.3 Kerberos认证技术	9.3.1 Kerberos简介	9.3.2 KerberosV4协议	9.3.3 KerberosV5简介	9.4 基于PKI的身份认证	9.4.1 PKI体系结构及各实体的功能	9.4.2 X.509证书	9.5 基于生物特征的身份认证	9.6 本章 小结习题																				
	第10章 访问控制	10.1 访问控制的概念	10.2 访问控制策略	10.2.1 自主访问控制模型	10.2.2 强制访问控制模型	10.2.3 基于角色的访问控制模型	10.3 访问控制策略的制定实施原则	10.4 访问控制的实现	10.4.1 访问控制的实现机制	10.4.2 网络中的访问控制	10.4.3 访问控制的实现手段	10.5 本章 小结习题																												
	第11章 防火墙技术	11.1 什么是防火墙	11.2 防火墙使用的技术	11.2.1 包过滤技术	11.2.2 电路级网关	11.2.3 应用层代理	11.2.4 网络地址转换	11.2.5 防火墙的性能比较	11.3 防火墙的主要作用	11.3.1 防火墙的基本功																														

能11.3.2 防火墙的扩展安全功能11.4 代理服务器CCPmxy11.4.1 CCProxy的安装11.4.2 ccPmxy的设置与管理11.4.3 客户端的配置11.4.4 CCPmxy的高级功能11.5 代理服务器squid11.5.1 squid的安装11.5.2 squid的配置11.5.3 squid的运行11.6 在Linux平台上使用iptables构建防火墙11.6.1 netfilter的工作原理11.6.2 系统准备11.6.3 iptables命令的语法11.6.4 使用iptables构建状态包过滤防火墙11.6.5 使用iptables构建状态NAT防火墙11.7 本章 小结习题第12章 入侵检测技术12.1 概述12.1.1 入侵检测的概念12.1.2 入侵检测的作用12.2 入侵检测系统12.2.1 入侵检测系统的模型12.2.2 入侵检测系统的工作流程12.2.3 入侵检测系统的分类12.2.4 入侵检测系统的部署12.3 入侵检测方法12.3.1 误用检测12.3.2 异常检测12.4 入侵检测面临的挑战与前景12.4.1 入侵检测面临的挑战12.4 入侵检测的前景12.5 入侵检测工具Snort12.5.1 Snort简介12.5.2 Snort的安装12.5.3 Snort的使用12.5.4 Snort的配置12.5.5 Snort的规则12.6 入侵检测实现示例12.6.1 开发环境的建立12.6.2 程序分析12.7 本章 小结习题参考文献

章节摘录

插图：

《计算机网络安全原理与实现》

编辑推荐

《计算机网络安全原理与实现》分为网络安全基础、网络安全中的攻击技术及网络安全中的防护技术三部分。先帮助读者补充网络协议、网络攻防编程方面的基础知识，再介绍网络攻击采取的手段，最后论述计算机网络的防护技术。《计算机网络安全原理与实现》既注重基本原理的讲解，又通过大量的例程演了相应的原理和技术；既对经典的、成熟的网络对抗技术做了详尽的介绍，又紧随网络对抗技术的研究前沿，涉猎了新理论、新技术和新方法，较为全面地反映了网络对抗技术的现状和发展趋势。随着信息化进程的加快，计算机网络的应用日益普及，但网络安全问题也不断凸显出来。《计算机网络安全原理与实现》以“计算机网络攻击和防护技术”为主线，系统介绍网络安全的原理和相关技术。

《计算机网络安全原理与实现》

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:www.tushu000.com