

<<计算机网络安全基础>>

图书基本信息

书名：<<计算机网络安全基础>>

13位ISBN编号：9787115093769

10位ISBN编号：7115093768

出版时间：2002-2

出版时间：第1版 (2002年2月1日)

作者：袁津生

页数：315

字数：493000

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>

<<计算机网络安全基础>>

内容概要

计算机网络安全是全社会都关注并亟待解决的一个大问题。如何保护自己的网络以及网络系统中的数据不被破坏和丢失，如何保证数据在传输过程中的安全，如何避免数据被篡改以及数据的真实性，是本书所阐述的问题。

本书重点介绍了与计算机系统安全有关的一些基础知识，如安全级别、访问控制、病毒和加密等。

本书可作为高等院校计算机专业教材，也可作为计算机网络的系统管理人员、安全技术人员的相关培训教材或参考书。

<<计算机网络安全基础>>

书籍目录

第1章 网络基础知识与因特网	11.1 网络参考模型OSI	1 1.1.1 分层通信	1 1.1.2 信息格式	2 1.2 网络互连
备	3 1.2.1 中继器和集线器	4 1.2.2 网桥	4 1.2.3 路由器	5 1.2.4 网关
802.3	7 1.3.2 令牌环网和IEEE 802.5	8 1.3.3 光纤分布式数据接口(FDDI)	9 1.4 广域网技术	10 1.4.1 广域网基本技术
11 1.4.2 广域网协议	14 1.5 TCP/IP协议基础	21 1.5.1 TCP/IP与OSI参考模型	22 1.5.2 网络层	24 1.5.3 传输层
30 1.5.4 应用层	33 1.6 因特网提供的主要服务	33 1.6.1 远程终端访问服务	33 1.6.2 传输服务	34 1.6.3 电子邮件服务
36 1.6.4 Usenet新闻服务	37 1.6.5 WWW服务	37 1.6.6 网络用户信息查询服务	38 1.6.7 实时会议服务	39 1.6.8 DNS服务
40 1.6.9 网络管理服务	40 1.6.10 NFS文件系统下的服务	44 1.6.11 X-Window服务	44 1.6.12 网络打印服务	44 1.7 小结
45 习题	46 第2章 操作系统与网络安全	47 2.1 Unix系统	47 2.1.1 Unix系统的由来	47 2.1.2 Unix常用命令介绍
48 2.1.3 Unix系统基本知识	49 2.2 Linux系统	51 2.2.1 Linux系统的由来	51 2.2.2 Linux的特点	51 2.2.3 vi用法介绍
52 2.2.4 gcc编译器和gdb调试器的使用	53 2.3 Windows系统	55 2.4 Unix网络配置	57 2.4.1 网络配置文件	57 2.4.2 Unix文件访问控制
59 2.4.3 NFS文件访问系统的安全	61 2.5 Windows NT网络配置	65 2.5.1 Windows NT的资源访问控制	65 2.5.2 Windows NT的NTFS文件系统	67 2.6 小结
68 习题	70 第3章 网络安全概述	71 3.1 网络安全基础知识	71 3.1.1 网络安全的含义	71 3.1.2 网络安全的特征
72 3.1.3 对网络安全的威胁	72 3.1.4 网络安全的关键技术	73 3.1.5 网络安全策略	74 3.2 威胁网络安全的因素	75 3.2.1 威胁网络安全的主要因素
75 3.2.2 各种外部威胁	77 3.2.3 防范措施	79 3.3 网络安全分类	81 3.4 网络安全解决方案	82 3.4.1 网络信息安全模型
83 3.4.2 安全策略设计依据	83 3.4.3 网络安全解决方案	84 3.4.4 网络安全性措施	89 3.4.5 因特网安全管理	92 3.4.6 网络安全的评估
92 3.5 小结	93 习题	94 第4章 计算机系统安全与访问控制	95 4.1 什么是计算机安全	95 4.2 安全级别
99 4.3 系统访问控制	101 4.3.1 系统登录	101 4.3.2 身份认证	106 4.3.3 怎样保护系统口令	107 4.3.4 关于口令维护的问题
109 4.4 选择性访问控制	111 4.5 小结	112 习题	113 第5章 数据库系统安全	114 5.1 数据库安全概述
114 5.1.1 简介	114 5.1.2 数据库的特性	114 5.1.3 数据库安全系统特性	115 数据库管理系统	116 5.2 数据库安全的威胁
117 5.3 数据库的数据保护	118 5.3.1 数据库的故障类型	118 5.3.2 数据库的数据保护	119 5.4 数据库备份与恢复	123 5.4.1 数据库备份的评估
123 5.4.2 数据库备份的性能	125 5.4.3 系统和网络完整性	126 5.4.4 制订备份的策略	126 5.4.5 数据库的恢复	127 5.5 小结
131 习题	132 第6章 计算机病毒的防治	134 6.1 什么是计算机病毒	134 6.2 计算机病毒的传播	135 6.2.1 计算机病毒的由来
135 6.2.2 计算机病毒的传播	135 6.2.3 计算机病毒的工作方式	136 6.3 计算机病毒的特点及破坏行为	139 6.3.1 计算机病毒的特点	139 6.3.2 计算机病毒的破坏行为
141 6.4 宏病毒及网络病毒	142 6.4.1 病毒	142 6.4.2 网络病毒	145 6.5 病毒的预防、检查和清除	147 6.5.1 病毒的预防
147 6.5.2 病毒的检查	153 6.5.3 计算机病毒的防治	153 6.5.4 计算机感染病毒后的恢复	154 6.5.5 计算机病毒的清除	155 6.6 病毒防御解决方案
157 6.6.1 多层次病毒防御的意义	158 6.6.2 Intel多层次病毒防御方案	158 6.6.3 KV3000杀毒软件简介	160 6.6.4 瑞星RISING99杀毒软件简介	164 6.7 小结
168 习题	170 第7章 数据加密	171 7.1 数据加密概述	171 7.1.1 密码学的发展	171 7.1.2 数据加密
172 7.1.3 基本概念	174 7.2 传统密码技术	179 7.2.1 密码表示方法	179 7.2.2 替代密码	180 7.2.3 换位密码
183 7.2.4 简单异或	184 7.2.5 一次密码本	185 7.3 数据加密	187 7.3.1 数据加密标准	187 7.3.2 国际数据加密算法
195 7.3.3 共享密钥技术的应用	195 7.4 公用密钥和私有密钥密码学	197 7.4.1 Diffie-Hellman密钥交换算法	197 7.4.2 RSA公用密钥/私有密钥	198 7.4.3 DES和RSA标准的比较
198 7.5 安全传输方法	199 7.6 验证	199 7.6.1 信息的验证	199 7.6.2 用户验证和证明权威	200 7.6.3 CA结构
200 7.7 加密软件PGP	201 7.8 小结	202 习题	204 第8章 防火墙技术	205 8.1 防火墙概念
205 8.1.1 因特网防火墙	205 8.1.2 数据包过滤	207 8.1.3 代理服务	208 8.1.4 防火墙体系结构	209 防火墙的各种变化和组合
213 8.1.6 内部防火墙	216 8.2 堡垒主机	219 8.2.1 建立堡垒主机的一般原则	219 8.2.2 堡垒主机的种类	219 8.2.3 堡垒主机的选择
220 8.2.4 堡垒主机提供的服务	222 8.2.5 建立堡垒主机	223 8.2.6 堡垒主机的监测	227 8.2.7 堡垒主机的保护与备份	227 8.3 包过滤
228 8.3.1 包过滤是如何工作的	228 8.3.2 包过滤路由器的配置	230 8.3.3 包的基本构造	231 8.3.4 包过滤处理内核	232 8.3.5 包过滤规则
236 8.3.6 依据地址进行过滤	237 8.3.7 依据服务进行过滤	239 8.4 代理服务	241 8.4.1 代理服务的优缺点	242 8.4.2 代理服务的工作方法
243 8.4.3 代理服务器的使用	244 8.4.4 使用代理的若干问题	245 8.4.5 关于因特网服务的代理特性	246 8.5 防火墙选择原则	250 8.6 小结
251 习题	253 第9章 网络站点的安全	253		

<<计算机网络安全基础>>

因特网的安全 254 9.1.1 因特网服务的安全隐患 254 9.1.2 因特网的脆弱性 256 9.2 Web站点安全 258 9.2.1
安全策略制订原则 258 9.2.2 配置Web服务器的安全特性 259 9.2.3 排除站点中的安全漏洞 260 9.2.4 监视
控制Web站点出入情况 261 9.3 黑客 262 9.3.1 黑客与入侵者 262 9.3.2 黑客攻击的三个阶段 263 9.3.3 对
黑客入侵 264 9.4 口令安全 266 9.4.1 口令破解过程 266 9.4.2 设置安全的口令 267 9.5 网络监听 267 9.5.1
监听的可能性 268 9.5.2 在以太网中的监听 268 9.5.3 网络监听的检测 270 9.6 扫描器 272 9.6.1 什么是扫
器 272 9.6.2 端口扫描 273 9.6.3 扫描工具 274 9.7 E-mail的安全 276 9.7.1 E-mail工作原理及安全漏洞 276
9.7.2 匿名转发 277 9.7.3 E-mail欺骗 277 9.7.4 E-mail轰炸和炸弹 278 9.7.5 保护E-mail 279 9.8 IP电子欺
骗 280 9.8.1 盗用IP地址 280 9.8.2 什么是IP电子欺骗 280 9.8.3 IP欺骗的对象及实施 281 9.8.4 IP欺骗攻
的防备 282 9.9 小结 283 习题 284 第10章 数据安全 285 10.1 数据完整性简介 285 10.1.1 数据完整性 285
10.1.2 提高数据完整性的办法 287 10.2 容错与网络冗余 288 10.2.1 容错技术的产生及发展 288 10.2.2 容
错系统的分类 289 10.2.3 容错系统的实现方法 290 10.2.4 网络冗余 293 10.3 网络备份系统 295 10.3.1 备
与恢复操作的种类 295 10.3.2 网络备份系统的组成 297 10.3.3 备份和恢复的设备与介质 301 10.3.4 磁带
轮换 303 10.3.5 备份系统的设计 304 10.3.6 备份的误区 307 10.4 小结 308 习题 309 附录 310 附录一 安全
安全站点 310 附录二 英文缩写词 312 参考文献 315

<<计算机网络安全基础>>

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>