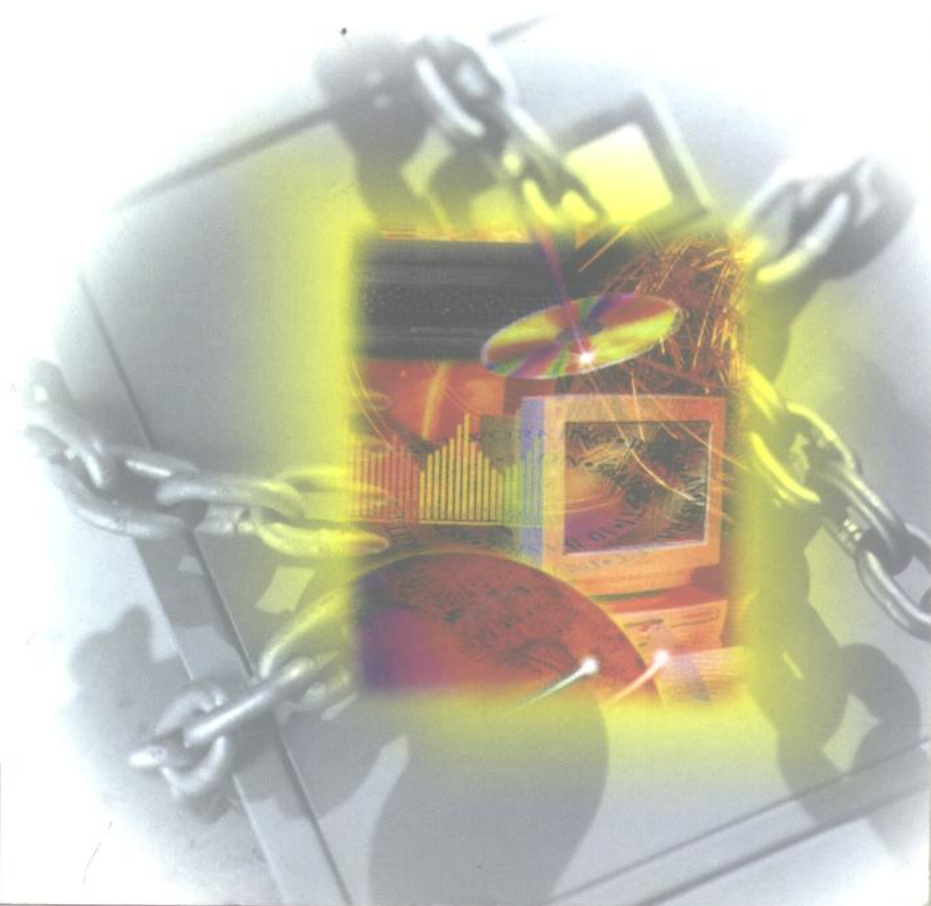


Network

网络

组建、管理与安全

张琳 李璇华 等编著
高徐娇 任晓娟



人民邮电出版社
www.pptph.com.cn

TP393
ZL/1

网络组建、管理与安全

张 琳 李璇华
高徐娇 任晓娟 等编著

人民邮电出版社

059447

图书在版编目 (CIP) 数据

网络组建、管理与安全/张琳等编著.—北京:人民邮电出版社,2000.12
ISBN 7-115-08836-5

I. 网... II. 张... III. 计算机网络—基本知识
IV. TP393

中国版本图书馆 CIP 数据核字 (2000) 第 75302 号

内 容 提 要

随着计算机及其网络日新月异的发展和普及,计算机网络带给人们的工作、生活以崭新的面貌。网络的规模不断扩大,网络的功能不断增强。广大计算机用户对计算机网络也给予了越来越多的关注。

本书从网络的基本概念、基本组成出发,先使读者对网络有个整体的认识,再与实际相结合,详细地介绍了 Windows NT、UNIX 和 NetWare 三个主要的网络操作系统的安装、配置和管理,还较为详细地介绍了网络安全方面的知识和相关技术。

本书适合于从事计算机网络设计和建设工作的技术人员,以及从事网络管理工作的人员阅读。

JS314/32

网络组建、管理与安全

- ◆ 编 著 张 琳 李璇华 高徐娇 任晓娟 等
责任编辑 王小明
- ◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 315@pptph.com.cn
网址 <http://www.pptph.com.cn>
北京汉魂图文设计有限公司制作
北京鸿佳印刷厂印刷
新华书店总店北京发行所经销
- ◆ 开本:787×1092 1/16
印张:46
字数:1149 千字
印数:1—5 000 册

2000 年 12 月第 1 版
2000 年 12 月北京第 1 次印刷

ISBN 7-115-08836-5/TP·1861

定价:66.00 元

目 录

第一章 网络概述	1
1.1 局域网与广域网	1
1.2 网络拓扑结构	2
1.2.1 星型网络拓扑	2
1.2.2 总线型网络拓扑	2
1.2.3 环型网络拓扑	3
1.3 以太网 II	3
1.3.1 以太网是怎样运作的	4
1.3.2 以太网介质	5
1.3.3 以太网帧格式	5
1.3.4 以太网寻址	6
1.3.5 以太类型	7
1.4 IEEE 局域网标准	7
1.4.1 IEEE 802 寻址	8
1.4.2 IEEE 802.2 逻辑链路控制	8
1.4.3 IEEE 802.3 CSMA/CD	10
第二章 OSI 参考模型	15
2.1 网络体系结构的基本概念	15
2.2 OSI 参考模型简介	16
2.2.1 OSI 参考模型层次划分原则	16
2.2.2 OSI 参考模型的结构	17
2.2.3 OSI 参考模型各层的主要功能	17
2.3 物理层	18
2.3.1 物理层概述	18
2.3.2 传输介质	19
2.3.3 物理接口的四个特性	23
2.3.4 物理接口标准	23
2.3.5 物理层常用的通信技术	27
2.4 数据链路层	29
2.4.1 数据链路层的基本概念	29
2.4.2 介质访问控制	31

2.4.3 寻址方式	34
2.4.4 传输同步	34
2.4.5 连接服务	37
2.4.6 面向比特型数据链路层协议 HDLC	38
2.5 网络层	43
2.5.1 网络层的基本功能	43
2.5.2 面向连接和无连接网络服务	44
2.5.3 寻址	44
2.5.4 交换技术	46
2.5.5 路由寻找	48
2.5.6 连接和网关服务	49
2.6 传输层	51
2.6.1 传输层在网络中的作用	51
2.6.2 传输层协议与网络层服务的关系	52
2.6.3 传输层的寻址	52
2.6.4 连接服务	53
2.6.5 传输层协议的分类	54
2.7 会话层	55
2.7.1 会话层概述	55
2.7.2 会话服务	55
2.7.3 会话层协议	57
2.8 表示层	59
2.8.1 表示层概述	59
2.8.2 表示层主要功能	60
2.8.3 表示服务	61
2.8.4 表示层协议	62
2.9 应用层	63
2.9.1 应用层概述	63
2.9.2 应用层的模型	63
2.9.3 应用层协议类型	63
第三章 常用网络协议	65
3.1 TCP/IP 协议簇	65
3.1.1 TCP/IP 协议概述	65
3.1.2 TCP/IP 协议模型	68
3.1.3 Internet 协议 IP	71
3.1.4 控制协议 TCP	75
3.1.5 TCP /IP 之上的网络服务和高层协议	77
3.2 NetWare 的协议 IPX/SPX	78
3.2.1 NetWare 和 OSI 的关系	78

3.2.2 网际分组交换协议 (IPX)	81
3.2.3 顺序包交换协议 (SPX)	84
3.2.4 NetWare 的核心协议 (NCP)	86
3.2.5 NetBIOS 的仿真	90
3.3 ATM 协议	93
3.3.1 ATM 的基本概念	93
3.3.2 ATM 协议参考模型	95
3.3.3 ATM 物理层	96
3.3.4 ATM 层	97
3.3.5 ATM 适配层	101
第四章 Windows NT 网的安装与配置	106
4.1 Windows NT 的安装	106
4.1.1 安装前的准备	106
4.1.2 分析和安排文件系统	108
4.1.3 在 Setup 进程中进行网络安装	110
4.1.4 对其他操作系统进行升级	112
4.1.5 从网络上进行安装	114
4.1.6 安装多重操作系统	115
4.1.7 在 RISC 系统上进行安装	115
4.2 网络的安装和配置	116
4.2.1 安装网络硬件	116
4.2.2 准备安装 TCP/IP	117
4.2.3 在 Windows NT 中安装和配置 TCP/IP	118
4.3 微软 Internet 信息服务器 (IIS)	122
4.3.1 了解 IIS	122
4.3.2 IIS 的安装	122
4.3.3 IIS 配置和管理	123
4.3.4 IIS 服务器的内容目录管理	125
4.3.5 IIS 安全问题	126
4.4 远程访问服务 (RAS)	127
4.4.1 RAS 概述	127
4.4.2 组建 RAS 网络	128
4.4.3 RAS 的 TCP/IP 设置	128
4.4.4 安装和配置 RAS 服务器	129
4.4.5 使用远程资源	132
第五章 Windows NT 网络的管理	134
5.1 Windows NT 的组	134
5.1.1 Windows NT 组的概念	134

5.1.2 Windows NT 的本地组 (Local Groups)	135
5.1.3 全局组 (Global Groups)	137
5.1.4 特殊组 (Special Groups)	137
5.2 域用户管理器	137
5.2.1 域 (Domain)	137
5.2.2 域用户管理器	138
5.2.3 用户的帐号管理	139
5.2.4 管理用户配置文件	145
5.3 资源管理器	147
5.3.1 资源管理器	147
5.3.2 资源管理器窗口的三种辅助工具	147
5.3.3 目录 (或文件) 的使用权	148
5.3.4 目录与文件的继承权	149
5.3.5 共享目录	150
5.4 服务器管理器	152
5.4.1 管理连接至某台计算机的用户	152
5.4.2 查看用户属性	153
5.4.3 管理某台计算机中的共享资源	155
5.5 打印机管理	155
5.5.1 “打印管理器”的窗口结构	155
5.5.2 建立一台网络打印机	155
5.5.3 连接至共享打印机	156
5.5.4 修改打印机的设置	157
5.5.5 赋予用户打印机的使用权限及实时管理	159
5.6 容错设计	160
5.6.1 磁盘管理器	160
5.6.2 Windows NT Server 的容错设计	161
第六章 Unix 网络的连接和配置	163
6.1 Unix 系统介绍	163
6.1.1 起源和历史	163
6.1.2 Unix 的特点	164
6.2 TCP/IP 连接	165
6.2.1 TCP/IP 简介	165
6.2.2 配置 TCP/IP 地址	166
6.2.3 TCP/IP 网络配置文件	167
6.2.4 网络守护进程——Daemon	169
6.2.5 建立用户替身	171
6.2.6 建立匿名 ftp	171
6.2.7 连接到 Internet	172

6.3 路由器	173
6.3.1 路由器的基本概念	173
6.3.2 维护和管理路由器	173
6.3.3 路由表的处理	175
6.3.4 指定路由器	175
6.3.5 子网技术	175
6.4 域名服务器 DNS	176
6.4.1 域名服务简介	176
6.4.2 建立域的准备工作的	177
6.4.3 在客户机上装备 DNS	178
6.4.4 在名字服务器上装备 DNS	180
6.5 邮件服务器	182
6.5.1 Unix 中用来处理邮件的软件系统	182
6.5.2 邮件系统环境的设置	182
6.6 配置 UUCP	183
6.6.1 UUCP 简介	183
6.6.2 UUCP 配置	184
6.7 网络文件系统 NFS	184
6.7.1 NFS 简介	184
6.7.2 NFS 安装和卸载	185
6.7.3 NFS 服务器的设置	185
6.7.4 NFS 客户机的设置	187
6.8 远程服务和文件传输	188
6.8.1 rlogin	188
6.8.2 telnet	189
6.8.3 rcp	190
6.8.4 ftp	190
6.8.5 其他命令	192
第七章 Unix 网络的管理	193
7.1 用户帐号管理	193
7.1.1 用户名和口令	193
7.1.2 注册和注销	193
7.1.3 用户组管理	194
7.1.4 用户管理	195
7.2 文件系统管理	198
7.2.1 文件系统类型	198
7.2.2 Unix 系统文件系统管理	200
7.2.3 NFS 的信息查询	204
7.3 网络与通信	205

7.3.1 网络配置文件	205
7.3.2 利用 Unix 邮件系统进行用户间通信	206
7.4 网络管理	210
7.4.1 ping 命令	210
7.4.2 ifconfig 命令	211
7.4.3 netstat 命令	211
7.4.4 运行软件检查	212
7.4.5 改进系统性能	212
7.5 安全管理	213
7.5.1 系统安全管理对策	213
7.5.2 小系统安全	213
7.5.3 系统管理员意识	217
7.6 调整及故障管理	219
7.6.1 进程管理	219
7.6.2 对系统性能进行监测	222
7.6.3 网络性能监测和调整	224
7.6.4 NFS 文件系统的故障诊断	225
第八章 Novell 网络的安装与配置	226
8.1 Novell 网络软件介绍	226
8.1.1 网络操作系统	226
8.1.2 客户软件	226
8.1.3 Novell 目录服务 (NDS)	227
8.1.4 实用工具程序	227
8.1.5 驱动程序	227
8.2 安装 NetWare 操作系统	227
8.2.1 从 NetWare 4.1x 升级	227
8.2.2 从 NetWare 3.1 升级	228
8.2.3 用 INSTALL 升级	228
8.2.4 用 Novell 升级向导 (Novell Upgrade Wizard) 升级	232
8.2.5 安装一台新的服务器	236
8.3 配置纯 IP 网络	241
8.3.1 网络规划	241
8.3.2 配置 TCP/IP 数据库文件	242
8.3.3 调整通信参数	248
8.3.4 配置并激活 TCP/IP	249
8.3.5 利用 INETCFG 进行网络配置	253
8.4 配置 NetWare 5 客户	257
8.4.1 Novell Client for Windows 95/98	257
8.4.2 NetWare 客户 for Windows NT	261

8.4.3 DOS 和 Windows 3.1x 的 NetWare 客户	263
8.5 配置 DNS 服务器	266
8.5.1 HOSTS 文件	266
8.5.2 介绍 DNS 服务器	267
8.5.3 为 NDS 添加 DNS 以及 DHCP 扩展	269
8.5.4 安装 DNS / DHCP 管理控制台	271
8.5.5 配置 DNS 客户端	271
8.5.6 配置 BIND 服务器数据库文件	272
8.5.7 交换 DNS 数据库	277
8.6 多协议路由器	278
8.6.1 配置 RIP 的 TCP/IP 加载参数	278
8.6.2 配置 RIP 的 TCP/IP 绑定参数	278
第九章 Novell 网的管理	281
9.1 NDS 介绍	281
9.1.1 目录与目录服务简介	281
9.1.2 介绍 NDS	281
9.1.3 NDS 特性和优点	283
9.1.4 支持 NDS 的两种强大工具	284
9.2 NDS 的管理	286
9.2.1 注册机制	286
9.2.2 ConsoleOne 启动序列与集合	287
9.2.3 Snap-in 类名	288
9.2.4 NDS 名字空间	288
9.3 用 ADSI 访问 NDS	288
9.3.1 ADSI 概述	288
9.3.2 捆绑到对象	289
9.3.3 ADSI 对象和接口	291
9.3.4 浏览 NDS 树	293
9.3.5 框架管理对象	293
9.4 目录和文件的权限	294
9.4.1 NetWare 的目录和文件权限	294
9.4.2 组合目录及文件权限	295
9.4.3 获取目录和文件权限的途径	296
9.5 目录和文件的属性	296
9.5.1 文件的属性	297
9.5.2 目录的属性	298
9.5.3 使用属性的规则	298
9.6 LDAP 服务器	299
9.6.1 Novell LDAP 服务器设计和配置	299

9.6.2 LDAP 开发环境综述	302
9.6.3 协议操作	303
9.7 管理 DNS 服务器	304
9.7.1 域名服务	304
9.7.2 管理域名服务 (DNS)	307
9.7.3 DNS 对象和 NDS	318
9.8 Novell 打印服务	319
9.8.1 Novell 分布式打印服务	319
9.8.2 打印服务的向后兼容性	322
9.8.3 使用 PCONSOLE 来配置打印服务	322
9.8.4 使用 NetWare Administrator 来配置打印服务	325
9.8.5 装载打印服务 (PSERVER.NLM)	326
第十章 现代广域网技术	328
10.1 广域网及相关概念	328
10.1.1 了解广域网的必要性	328
10.1.2 广域的定义	328
10.2 广域网的基本实现模式	332
10.2.1 采用传统的 PSTN 方式	332
10.2.2 采用 X.25 网 (数据交换网)	332
10.2.3 采用 ISDN 网	334
10.2.4 ATM 技术	339
10.2.5 帧中继	342
10.2.6 采用 DDN 技术	346
10.2.7 采用 VPN (虚拟专用网)	347
10.3 广域网的管理	351
10.3.1 网络优化	351
10.3.2 流量管理	351
10.3.3 故障处理	352
10.3.4 安全管理	352
第十一章 网络互联的技术与实现	354
11.1 网络互联问题的提出	354
11.1.1 网络互联的必要性	354
11.1.2 网络互联设计与实现的基本原则	354
11.2 异种网络互联技术	355
11.2.1 基本技术介绍	355
11.2.2 三种网络操作系统的比较	357
11.2.3 Windows NT 与 NetWare 的互联	357
11.2.4 Windows NT 与 Unix 的互联	360

11.2.5 Unix 与 NetWare 的互联	366
11.3 现代网络互联技术	370
11.3.1 ATM 与异种网络互联	370
11.3.2 ATM 与 Internet 互联	374
11.3.3 ISDN 与 LAN 远程互联	377
第十二章 网络安全对策	382
12.1 TCP/IP 基础	382
12.1.1 IP 报头	382
12.1.2 TCP 头格式	383
12.1.3 TCP 传输原理	384
12.2 IP 欺骗	384
12.2.1 信任关系	385
12.2.2 TCP 序列号预测	385
12.2.3 IP 欺骗	386
12.2.4 使被信任主机丧失工作能力	387
12.2.5 序列号取样和猜测	388
12.2.6 IP 欺骗的防止	388
12.3 防火墙	389
12.3.1 防火墙概念	389
12.3.2 采用防火墙的必要性	390
12.3.3 防火墙的构成	392
12.3.4 网络政策	392
12.3.5 先进的验证	393
12.3.6 包过滤	394
12.4 Unix 系统安全管理	396
12.4.1 安全管理	397
12.4.2 超级用户	397
12.4.3 文件系统安全	397
12.5 NT 安全	402
12.5.1 NT 服务器和工作站的安全漏洞	402
12.5.2 NT 管理员对策	409
第十三章 网络安全分析和安全策略	413
13.1 网络安全基础知识	413
13.1.1 网络安全的含义	413
13.1.2 计算机安全的正式分级	414
13.1.3 网络安全模型结构	417
13.1.4 安全服务的层次配置	419
13.1.5 网络安全的安全策略	421

13.1.6 网络安全技术现状	423
13.1.7 网络安全不容忽视	426
13.2 Internet 上的危险和安全缺陷	428
13.2.1 因特网的危险概述	428
13.2.2 因特网不安全的原因	429
13.2.3 TCP/IP 协议的安全缺陷	429
13.2.4 TCP/IP 协议常见的攻击方式	431
13.3 TCP/IP 协议各层的安全性分析	436
13.3.1 Internet 层的安全性	437
13.3.2 传输层的安全性	441
13.3.3 应用层的安全性	442
13.4 信息安全技术概论	444
13.4.1 信息安全技术与网络安全	444
13.4.2 信息安全模型与主要技术	445
13.4.3 信息安全系统设计原则	447
13.4.4 信息安全系统的设计与实现	449
第十四章 Unix 系统安全	452
14.1 Unix 网络不安全的因素	452
14.1.1 特权软件的安全漏洞	452
14.1.2 研究源码的漏洞	454
14.1.3 特洛伊木马	454
14.1.4 网络监听及数据截取	454
14.1.5 软件之间相互作用和设置	454
14.2 Unix 系统安全的基本概念	455
14.2.1 Unix 系统的基本知识	455
14.2.2 用户的安全	458
14.2.3 程序员的安全性	461
14.3 以网络黑客的身份检查 Unix 系统的安全性	465
14.4 Unix 系统的安全措施	477
14.4.1 口令和帐号安全	477
14.4.2 文件系统安全	479
14.4.3 X Windows 的安全性	479
14.4.4 网络安全措施	481
第十五章 Windows NT 系统安全	484
15.1 Windows NT 系统概述	484
15.1.1 Windows NT 术语介绍	484
15.1.2 Windows NT 环境配置	487
15.2 Windows NT 的安全机制	491

15.2.1 Windows NT 的安全概述	491
15.2.2 Windows NT 安全模型	494
15.3 Windows NT 已知的安全漏洞	498
15.3.1 破坏 NT 安全的工具	498
15.3.2 NT 系统下的其他安全漏洞	499
15.4 Windows NT 的安全性评估	506
15.4.1 审查系统是否遵从 C2 安全级	506
15.4.2 标准评估	507
15.4.3 帐户策略和限制	507
15.4.4 用户帐户	507
15.4.5 组	508
15.4.6 管理员帐户和管理员组	508
15.4.7 Guest 级帐户和 everyone 组	509
第十六章 Web 系统安全	510
16.1 Web 结构简介	510
16.1.1 Web 服务器	510
16.1.2 Web 浏览器	510
16.1.3 通用网关接口 (CGI)	511
16.1.4 cookies	511
16.2 Web 安全性的框架	512
16.2.1 如何实施 Web 安全框架	513
16.2.2 Web 服务提供者的风险和安全提升机制	514
16.2.3 如何保护 Web 站点上的机密数据	518
16.2.4 Web 客户的风险和安全提升机制	520
16.2.5 Web 浏览器的安全漏洞及解决方案	523
16.3 CGI 脚本的安全性	525
16.4 Cookies 的安全性	528
16.5 Java 的安全性	530
第十七章 加密与认证技术	534
17.1 密码学的基本概念	534
17.1.1 现代密码学基础	535
17.1.2 分组密码和序列密码	536
17.1.3 公钥密码体制	537
17.1.4 密码分析	539
17.2 信息加密技术	542
17.2.1 保密通信模型	542
17.2.2 数据加密技术	543
17.3 对称密钥加密体制	545

17.3.1 DES 算法	545
17.3.2 IDEA 算法	546
17.3.3 LOKI 算法	546
17.4 非对称密钥加密体制及数字签名	547
17.4.1 RSA 公钥体制	547
17.4.2 Elgamal 公钥体制	548
17.4.3 Knapsack 公钥体制	548
17.4.4 DH 公钥分配密码体制	548
17.4.5 其他加密技术	548
17.5 加密技术应用——PGP 工具	550
17.5.1 PGP 概述	550
17.5.2 PGP 的机制	551
17.5.3 PGP 软件使用介绍	554
17.5.4 PGP 的安全性分析	558
17.5.5 RSA 的攻击方法	560
17.5.6 PGP 攻击	562
17.6 信息认证技术	563
17.6.1 消息认证	563
17.6.2 身份认证	566
17.6.3 数字签名	568
第十八章 防火墙设计	571
18.1 防火墙基础知识	571
18.1.1 引入防火墙的好处	572
18.1.2 防火墙模型与安全策略	574
18.1.3 防火墙的主要组成部分	579
18.1.4 防火墙的缺陷	586
18.2 防火墙结构	588
18.2.1 双重宿主主机的概念及服务方式	588
18.2.2 被屏蔽主机	592
18.2.3 被屏蔽子网	595
18.3 堡垒主机	597
18.3.1 堡垒主机基础知识	597
18.3.2 设计和构筑堡垒主机的基本原则	598
18.3.3 配置和保护堡垒主机	598
18.3.4 堡垒主机的维护	599
18.4 防火墙测试	600
18.4.1 端口扫描	600
18.4.2 在线监测	601
18.4.3 系统日志审核	602

第十九章 网络安全扫描工具	604
19.1 扫描工具概述	604
19.1.1 扫描工具的工作原理	604
19.1.2 一个简单的端口扫描程序	607
19.1.3 扫描工具的重要性	610
19.2 ISS	611
19.2.1 ISS 的功能	611
19.2.2 ISS (Internet Security Scanner) 使用说明	613
19.2.3 ISS 应用举例	615
19.3 SATAN	616
19.3.1 SATAN 介绍	617
19.3.2 安装 SATAN 软件包	617
19.3.3 使用 SATAN 软件包	619
19.4 其他扫描工具	621
19.4.1 NSS (Network Security Scanner)	621
19.4.2 SAFESuite	622
19.4.3 Strobe	623
19.4.4 COPS (Computer Oracle and Password System)	625
19.4.5 Internet Scanner	627
19.4.6 trojan.pl	628
19.4.7 Jakal	628
19.4.8 IndentTCPscan	628
19.4.9 Test Hosts For Well-Known NFS Problems/Bugs	629
19.4.10 SPI (Security Profile Inspector)	629
19.4.11 CONNECT	629
19.4.12 FSPScan	629
19.4.13 XSCAN	629
19.4.14 Secure_Sun	630
19.4.15 Doc (Domain Obscenity Control)	630
19.4.16 Check Xusers	630
19.4.17 Crashme	630
19.4.18 Port Scanner	630
19.5 端口扫描中的一些技巧	632
第二十章 网络监听及审计监测工具	634
20.1 网络监听基本知识	634
20.1.1 网络监听定义	634
20.1.2 网络监听的作用	636
20.2 系统本身提供的一些工具	639

20.2.1 find 命令	640
20.2.2 netstat 命令	640
20.3 网络监听工具	641
20.3.1 snoop	642
20.3.2 Sniffit 软件	643
20.4 检测和分析工具	646
20.4.1 NetXRay 协议分析和网络监控软件	646
20.4.2 Tripwire	649
20.4.3 其他监测和分析工具	651
20.5 系统状态报告工具	654
20.5.1 Icmpinfo	654
20.5.2 CPM (Check Promiscuous Mode)	656
20.5.3 ident	656
20.5.4 Ifstatus	656
20.5.5 EtherBoy	657
20.5.6 PacketBoy	657
20.5.7 WebSENSE	658
20.5.8 LAN Watch	658
20.6 审计与日志工具	658
20.6.1 大多数 Unix 操作系统中的日志文件	659
20.6.2 Authd (Authentication Server Daemon)	659
20.6.3 dump_lastlog	660
20.6.4 Logging fingerd in PERL	660
20.7 实时攻击响应工具	660
20.7.1 Dummy “su” program	660
20.7.2 Fack-rshd	660
20.7.3 Rsucker	660
20.7.4 Watchdog.com	660
20.8 访问控制工具	661
20.8.1 网络访问控制验证工具	661
20.8.2 单机访问控制工具	662
第二十一章 基于防火墙的安全 Internet 工具	665
21.1 名字服务器和防火墙的配合	665
21.1.1 名字服务器的代理特性	665
21.1.2 分散的名字服务器策略	666
21.1.3 非透明防火墙网络的名字服务器	669
21.1.4 透明防火墙的名字服务器	671
21.2 穿越防火墙的远程执行和远程登录	674
21.2.1 远程命令执行	674