

192.168.168.168

110.103.96.22

192.168.168.1

255.255.255.0

192.168.168.168

110.103.96.22

192.168.168.1

255.255.255.0

192.168.168.168

110.103.96.22

192.168.168.1

255.255.255.0

192.168.168.168

110.103.96.22

192.168.168.1

255.255.255.0

192.168.168.168

110.103.96.22

192.168.168.1

255.255.255.0

110.103.96.22

192.168.168.1

255.255.255.0

192.168.0.1

202.96.168.68

192.168.168.168

110.103.96.22

192.168.168.1

255.255.255.0

192.168.0.1

202.96.168.68

192.168.168.168

110.103.96.22



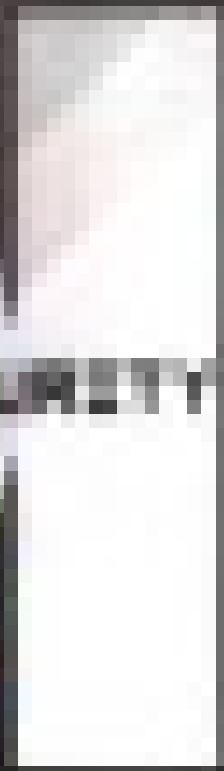
WEBSERVER SECURITY

网络服务器 安全配置详解

网络安全专家
EXPERT

刘志勇 郭聪辉 编著
飞思科技产品研发中心 监制

电子工业出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn



2015年10月 第10期
第10期

网络安全专家

网络服务器安全配置详解

刘志勇 郭聪辉 编著

飞思科技产品研发中心 监制

电子工业出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

本书以介绍网络服务器的安装和安全性配置等相关知识为主，针对时下三大主流操作系统：Linux、Windows 2000 Server 和 FreeBSD，详细介绍了它们的特点、性能和安装方法，讲解了相关的安全问题，以及如何如何进行安全配置和日常管理等内容。书中提供了翔实的案例和操作细节。通过本书的阅读，读者能够在企业网、校园网等实际应用中根据系统需求制定出有效的安全措施以实现网络系统的安全与管理。

本书适合系统管理员、网络管理员及对网络与系统安全感兴趣的计算机爱好者阅读。

未经许可，不得以任何方式复制或抄袭本书的部分或全部内容。

版权所有，侵权必究。

图书在版编目(CIP)数据

网络服务器安全配置详解 / 刘志勇, 郭聪辉编著. —北京: 电子工业出版社, 2004.3

(网络安全专家)

ISBN 7-5053-9504-1

I.网... II.①刘...②郭... III.网络服务器—安全技术 IV.TP368.5

中国版本图书馆 CIP 数据核字 (2003) 第 119896 号

责任编辑: 杨 鸥

印 刷: 北京东光印刷厂

出版发行: 电子工业出版社

北京海淀区万寿路 173 信箱 邮编: 100036

经 销: 各地新华书店

开 本: 787×1092 1/16 印张: 27 字数: 691.2 千字

印 次: 2004 年 3 月第 1 次印刷

印 数: 5 000 册 定价: 36.00 元

凡购买电子工业出版社的图书, 如有缺损问题, 请向购买书店调换。若书店售缺, 请与本社发行部联系, 联系电话: 010-68279077。质量投诉请发邮件至 zlts@phei.com.cn, 盗版侵权举报请发邮件至 dbqq@phei.com.cn。

前 言

21 世纪，信息化浪潮如日中天，它描绘了新世纪 e 时代的壮丽画卷。计算机网络信息技术如黄河之水天上来，不管人们对信息化持什么样的态度，我们都不得不迎接它汹涌而至的浪潮。

在 20 世纪 80 年代，随着网络进一步平民化、商业化，最终，它提供了自 20 世纪 50 年代以来的新信息革命后的一次伟大转机，计算机网络逐步取代电脑成为信息社会的技术核心，也就是说，电脑是网络的终端，网络并不是电脑的外围。这一革命性的变化演绎出了网络时代的意义，网络不仅能够传递信息，还能在信息存储和转换、信息处理和信息收发等方面扩展自身的功能。放眼全球，Internet 几乎遍及世界上每一个角落，由 60 多万个网络、几千万台主机组成，为上亿用户提供多样化的网络和信息服务。在信息化社会，网络信息系统已经在政治、电信、商业、金融、工业、文教、军事、交通等各方面发挥着越来越大的作用，现今社会对计算机网络信息系统的依赖程度也日益增加。

得益于网络信息系统的不断完善，敏感信息和无形财富日趋高度集中于计算机中。网络信息系统依靠计算机网络接收和处理信息，从而达到其相互间的联系和对目标的管理、控制的目的。现代信息社会的一个重要特征是以网络方式获得、交流信息。网络正在以前所未有的规模改变着人们的工作和生活方式。

随着网络的开放性、共享性、互联性的进一步扩大，特别是 Internet 的出现，以及 Internet 之后出现的 Intranet，网络的重要性和对社会的影响越来越凸现出来。网络上各种新业务的兴起，如电子商务、电子出版、数字图书馆、电子货币等，这些网络信息技术给人们带来了便利，但也留下了许多安全隐患，如病毒、黑客活动等的攻击和破坏，造成信息的泄密和巨大的经济损失，信息安全问题在今天已经成为关注的焦点。

很多组织现有的计算机网络大多数在建设之初都忽略了安全问题，即便考虑了这个问题，也只是简单地把安全机制建立在物理安全机制上，因此，随着网络的规模日趋扩大，这种安全机制对于网络环境来说就越来越形同虚设。另外，目前网络所使用的协议，在制定之初没有考虑安全方面的要求，自然也就没有安全性可言。计算机网络安全问题的主要根源就是其开放性和资源共享。它的安全性主要依赖加密、网络用户身份鉴别、存取控制策略等技术手段。

面对日趋严重危害网络系统的种种威胁，安全与保密的重要性要求越来越迫切，必须采取有力措施保证网络信息安全，满足保密的需要。一般来讲，网络安全措施分为三类：逻辑上的、物理上的和政策上的。仅仅利用物理上和政策上的手段防范黑客入侵，显得方法十分有限，实施也有一定困难。因此，必须高度重视采用逻辑上的措施，也就是运用网络安全技术保证安全。

即使有了非常完备的安全与保密的政策法规和非常先进的安全与保密技术，以及天衣无缝的物理安全机制，但如果这些得不到普及和应用，那么所有的努力都是白费。

服务器是网络信息系统的核心，其重要性不言而喻。一旦服务器被攻破，那么整个网络信息系统就暴露在光天化日下了。

在目前的网络系统中，核心是网络服务器操作系统，因此，操作系统的安全与否直接决定着信息是否安全，必须考虑主机的安全性问题。为此，电子工业出版社飞思科技产品研发中心

策划了这本书，以介绍时下主流网络服务器的安装和有关安全性方面的配置为主，针对实际威胁安全的因素，给出具体有效的解决方案，以达到网络整体安全的目的。本书分三部分，第一部分是 Linux 篇，第二部分是 Windows 2000 Server 篇，第三部分是 FreeBSD 篇。本书由刘志勇、郭聪辉主笔，李雪松、雷向利、刘峰、朱国伟、饶思贤、薛引峰等人参与了编写。由于作者水平有限，书中难免出现各种失误和不当，欢迎大家批评指正。

我们的联系方式：

咨询电话：(010) 68134545 68131648

答疑邮件：support@fecit.com.cn

网 址：<http://www.fecit.com.cn> <http://www.fecit.net>

答疑网址：<http://www.fecit.com.cn/>下的“问题解答”专区

通用网址：计算机图书、FECIT、飞思教育、飞思科技、飞思

飞思科技产品研发中心

目 录

Linux 篇

第 1 章 UNIX 世界初探.....	3	3.3 账户安全.....	45
1.1 UNIX 简介.....	3	3.3.1 用户的管理.....	45
1.2 UNIX 世界的新秀——Linux.....	4	3.3.2 用户组的管理.....	47
1.3 Linux 的特性.....	5	3.3.3 传统口令和影子口令的 相互转换.....	48
1.4 Linux 与 Windows NT/2000 Server 的安全性能比较.....	6	3.3.4 验证口令、组和相应的 影子文件.....	49
1.5 相关名词与命令.....	8	3.3.5 防止任何用户使用 su 命令 变为超级用户 root.....	49
1.5.1 启动.....	8	3.3.6 用户自动注销.....	49
1.5.2 常用的一些命令.....	8	3.4 文件系统安全.....	50
第 2 章 拥抱 Linux.....	11	3.4.1 文件访问权限.....	50
2.1 Linux 的硬件需求.....	11	3.4.2 目录许可.....	51
2.2 Linux 的安装方式.....	12	3.4.3 设置账户和组账户的权限.....	51
2.3 Linux 的安装.....	13	3.5 网络安全.....	52
2.3.1 安装前的准备.....	13	3.5.1 Linux 提供的网络服务 及安全管理.....	52
2.3.2 设置硬盘分区.....	14	3.5.2 具有潜在安全风险的服务.....	58
2.3.3 安装 Linux.....	18	3.6 Linux 系统和网络安全忠告.....	60
2.3.4 安装之后.....	29	3.6.1 系统管理员面临的基本 安全问题.....	60
2.4 Linux 使用技巧.....	30	3.6.2 用户基本安全问题.....	61
2.4.1 如何建立多用户.....	30	3.6.3 其他安全问题.....	65
2.4.2 使用软盘、光盘及 DOS 等非 Linux 分区.....	30	3.6.4 保持账户安全的要点.....	66
2.4.3 如何安装 Linux 的应用软件.....	31	第 4 章 Web 服务器王中王——Apache.....	69
2.4.4 如何设置声卡.....	32	4.1 WWW 简介.....	69
2.4.5 如何设置显卡.....	32	4.1.1 WWW 的渊源.....	69
2.4.6 Linux 的文件操作.....	33	4.1.2 WWW 的特点.....	69
2.4.7 如何在 Windows 系统中查看 Linux 文件.....	33	4.1.3 WWW 的结构.....	70
2.4.8 Linux 的启动与运行.....	34	4.2 Apache 服务器简介.....	70
2.4.9 Linux 其他常用技巧.....	35	4.2.1 Apache 的由来.....	70
第 3 章 确保 Linux 系统的安全.....	39	4.2.2 Apache 的官方下载地址.....	71
3.1 Linux 系统的安全性.....	39	4.2.3 Apache 与其他 WWW 服务器 的比较.....	71
3.2 基本安全.....	39		
3.2.1 开机安全.....	39		
3.2.2 口令安全.....	42		

4.3	Apache 的安装.....	72	5.3.3	FTP 的口令及用户组文件	112
4.3.1	检查系统中是否存在 Apache 及其版本	72	5.3.4	FTP 服务器的系统安全	112
4.3.2	不带 SSL 的 Apache 的安装	73	5.4	wu-ftpd 的应用技巧	113
4.3.3	带 SSL 的 Apache 的安装	73	第 6 章	E-mail 服务器	117
4.4	Apache 的启动和停止	74	6.1	E-mail 简介	117
4.5	Apache 的设置	75	6.1.1	E-mail 程序的分类	118
4.5.1	Apache 的配置文件	75	6.1.2	MTA 程序	118
4.5.2	Apache 设置目录级访问控制	82	6.2	SendMail 的配置	118
4.5.3	Apache 中 SSI 的设置	83	6.2.1	SendMail 简介	118
4.5.4	在 Apache 上运行 CGI	85	6.2.2	SendMail 的获取	119
4.6	Apache 的日志文件	87	6.2.3	SendMail 的安装	119
4.6.1	访问日志	87	6.2.4	SendMail 的设置	121
4.6.2	错误日志	89	6.2.5	sendmail.cf 与 m4	125
4.6.3	定制日志	90	6.2.6	SendMail 服务实战	128
4.6.4	日志分析	91	6.3	SendMail 的安全	132
4.7	安全的 Apache 服务器	92	6.3.1	加强 SendMail 的 DoS 抗击能力	132
4.7.1	Apache 的主要缺陷	92	6.3.2	SendMail 与文件系统的安全	133
4.7.2	加强 Apache Web 服务器的安全	93	6.3.3	mc 文件的 FEATURE 命令与网络安全	134
4.8	Apache 服务器的应用技巧	94	6.3.4	藏匿 SendMail 的版本信息	136
4.9	总结	97	6.3.5	防止 SendMail 被未授权用户滥用	136
第 5 章	FTP 服务器至尊——wu-ftpd	99	第 7 章	炼就火眼金睛——日志分析的应用	137
5.1	FTP 服务简介	99	7.1	Linux 日志系统	137
5.1.1	FTP 的特征	99	7.2	RedHat Linux 常见的日志文件	137
5.1.2	FTP 的工作方式	99	7.2.1	RedHat Linux 常用的日志文件	138
5.1.3	FTP 的访问方式	100	7.2.2	具体命令	141
5.2	通用 FTP 服务器简介——wu-ftpd	100	7.2.3	进程统计	143
5.2.1	wu-ftpd 的获取	100	7.2.4	syslog 设备	145
5.2.2	wu-ftpd 的安装	101	7.2.5	程序日志与其他	147
5.2.3	wu-ftpd 的设置	103	7.3	配置日志文件	147
5.2.4	wu-ftpd 的工具	107	7.3.1	/etc/syslog.conf 的格式	148
5.3	保证 wu-ftpd 服务器的安全	108			
5.3.1	wu-ftpd 的安全问题	108			
5.3.2	有关目录访问权限	110			

7.3.2	将日志文件记录到远程主机.....	149
7.3.3	将警告信息发送到控制台	149
7.4	利用日志文件.....	150
7.5	分析日志文件.....	150
第 8 章	系统安全的堡垒	
	——文件系统与系统加固.....	153
8.1	Linux 日志式文件系统.....	153
8.1.1	ext2 文件系统的安全.....	154
8.1.2	ext3 日志文件系统.....	158
8.1.3	XFS 文件系统.....	160
8.1.4	ReiserFS 文件系统.....	163
8.1.5	GFS 文件系统.....	165
8.2	Linux 系统深度安全加固.....	166

Windows 2000 Server 篇

第 9 章	Windows 的历史.....	175
9.1	Windows 2000 的前身.....	175
9.2	Windows 2000 的产品定位.....	178
9.3	Windows 2000 的发展策略.....	178
9.4	Windows 2000 的家族.....	179
9.4.1	Windows 2000 Professional.....	179
9.4.2	Windows 2000 Server.....	179
9.4.3	Windows 2000 Advanced Server.....	179
9.4.4	Windows 2000 Datacenter Server.....	180
9.5	Windows 2000 Server 的功能.....	180
第 10 章	你好, Windows 2000 Server.....	183
10.1	Windows 2000 Server 的硬件需求.....	184
10.2	安装 Windows 2000 Server 之前的规划.....	186
10.2.1	安装的方式.....	186
10.2.2	采用何种文件系统.....	187
10.2.3	是否保留多重系统引导模式.....	188

10.2.4	选择安装的组件.....	188
10.3	Windows 2000 Server 的安装方式.....	188
10.3.1	光盘引导安装.....	188
10.3.2	软盘引导安装.....	188
10.3.3	运行安装程序.....	188
10.3.4	从网络上安装.....	189
10.4	安装 Windows 2000 Server.....	189
10.5	软硬件安装.....	195
第 11 章	Windows 2000 Server 本地安全..	197
11.1	打开审核功能.....	197
11.2	关闭一切不必要的端口.....	197
11.2.1	关闭 TCP/UDP 端口 135 ~ 139 和 445.....	198
11.2.2	关注 TCP 3389 端口.....	200
11.2.3	警惕 UDP 161 端口.....	205
11.2.4	关注 TCP/UDP 389、3268 端口.....	209
11.3	修改注册表加强 Windows 2000 Server 本地的安全性.....	210
11.4	安全配置 Windows 2000 Server.....	212
11.4.1	端口设置.....	213
11.4.2	IIS 配置.....	213
11.4.3	账号安全.....	214
11.4.4	安全日志.....	214
11.4.5	目录和文件权限.....	215
11.4.6	预防 DoS.....	216
11.4.7	需要注意的一些事.....	216
11.5	Windows 2000 的服务安全与建议.....	218
第 12 章	易用为王——IIS 5.0.....	225
12.1	IIS 简介.....	225
12.2	IIS 的特色.....	225
12.3	IIS 的安装.....	225
12.4	IIS 的安全设置.....	229
12.4.1	以 Windows NT 的安全机制为基础.....	229

12.4.2	安装时应注意的安全问题.....	230	13.5	Serv-U FTP Server 本地提升 权限缺陷.....	263
12.4.3	IIS 对 IP 地址和域名的限制.....	230	13.5.1	测试方法.....	264
12.4.4	IIS 权限的设置.....	231	13.5.2	漏洞分析.....	264
12.4.5	IIS 身份验证.....	232	第 14 章	忠实的邮差——IMail Server	267
12.4.6	访问权限控制.....	234	14.1	IMail Server 简介.....	267
12.4.7	端口安全性的实现.....	234	14.2	IMail Server 安装.....	267
12.4.8	IP 转发的安全性.....	234	14.3	建立邮件服务器.....	268
12.4.9	SSL 安全机制.....	235	14.3.1	建立邮件服务器.....	268
12.5	加固 IIS 的第三方工具.....	235	14.3.2	建立信箱.....	269
12.5.1	SecureIIS.....	235	14.3.3	增加邮件服务器.....	271
12.5.2	URLScan.....	236	14.4	IMail 的 Web 登录.....	272
12.5.3	IIS Lockdown Tool.....	238	14.5	以 Web 方式收发邮件.....	275
12.6	IIS 的排错.....	240	14.5.1	关于 Web 方式.....	275
12.6.1	重新启动 IIS.....	240	14.5.2	Web 方式的基本操作.....	275
12.6.2	IIS 的备份与还原.....	242	14.6	无 IP 地址的虚拟邮件主机.....	277
12.7	IIS 的日志分析.....	242	14.6.1	DNS 设置.....	277
12.8	堵住 IIS 的漏洞.....	247	14.6.2	IMail Administrator 设置... ..	278
12.9	IIS 的 FTP 安全设置.....	248	14.6.3	使用（以在 Outlook 中 为例）.....	278
第 13 章	傻瓜式的 FTP 服务器 ——功能强大的 Serv-U.....	253	14.7	有 IP 地址的虚拟邮件主机.....	279
13.1	Serv-U 简介.....	253	14.7.1	DNS 的设置.....	279
13.2	Serv-U 的安装和卸载.....	253	14.7.2	IMail 的设置.....	280
13.2.1	Serv-U 的安装.....	254	14.8	IMail 之邮件列表.....	280
13.2.2	Serv-U 的卸载.....	255	14.8.1	建立和使用邮件列表.....	280
13.3	建立第一个 FTP 服务器.....	255	14.8.2	基本设置.....	281
13.3.1	设置 Serv-U 的 IP 地址... ..	255	14.8.3	邮件列表的其他设置.....	282
13.3.2	设置 FTP 服务器域名.....	256	14.9	IMail 的别名.....	283
13.3.3	设置匿名登录.....	256	14.9.1	主机别名的建立.....	283
13.3.4	创建新账户.....	257	14.9.2	邮箱别名的建立.....	283
13.4	Serv-U 常见基本操作.....	259	14.9.3	使用邮箱别名.....	284
13.4.1	管理员设置.....	259	14.10	IP 地址变更.....	284
13.4.2	客户端的连接.....	261	第 15 章	Windows 2000 Server 的系统日志 的管理	287
13.4.3	对 FTP 用户的管理.....	261	15.1	Windows 日志概述.....	287
13.4.4	对目录权限的管理.....	262	15.2	事件的类型.....	288
13.4.5	增加虚拟目录.....	263	15.3	系统日志的管理、安全配置.....	289
			15.4	日志的备份与查询.....	291

第 16 章 更上一层楼——Windows 2000	
Server 系统加固.....	293
16.1 系统安全从安装开始.....	293
16.2 关闭服务减少风险.....	294
16.3 文件与目录管理.....	295
16.3.1 Web 目录设置.....	295
16.3.2 文件权限设置.....	296
16.4 企业服务器配置.....	297
16.4.1 迁移应用程序.....	297
16.4.2 策略设置与 IP 地址过滤..	298
16.4.3 日志设置.....	301
16.4.4 注册表加系统安全.....	301
16.4.5 FTP 服务限制.....	302
16.4.6 SQL 优化.....	303
16.4.7 脚本安全.....	304
FreeBSD 篇	
第 17 章 FreeBSD 的渊源.....	309
17.1 FreeBSD 的渊源.....	309
17.2 FreeBSD 的家族.....	311
17.3 FreeBSD 的特性.....	312
17.4 FreeBSD 的应用范围.....	313
第 18 章 接近神秘的 FreeBSD.....	315
18.1 安装前的准备工作.....	315
18.1.1 安装 FreeBSD 的硬件需求.....	315
18.1.2 FreeBSD 系统的安装方式.....	317
18.1.3 准备启动安装软盘.....	319
18.2 FreeBSD 安装.....	322
18.2.1 启动安装内核程序.....	322
18.2.2 为 FreeBSD 准备硬盘空间.....	323
18.2.3 指定硬盘标签.....	324
18.2.4 选择安装内容.....	326
18.2.5 选择安装媒介.....	326
18.2.6 确认安装.....	327
18.3 FreeBSD 的启动与关闭.....	328
18.3.1 启动过程.....	328
18.3.2 登录系统.....	329
18.3.3 关闭系统.....	329
18.4 认识 FreeBSD 文件系统.....	330
18.4.1 文件系统的结构.....	331
18.4.2 关于分区.....	332
18.4.3 如何使用其他分区.....	332
18.5 FreeBSD 的网络配置.....	333
18.5.1 配置计算机名字.....	333
18.5.2 配置网络界面.....	333
18.5.3 配置路由表.....	334
18.5.4 保存配置.....	335
18.5.5 基本网络工具的使用.....	335
18.6 Ports 和 Package.....	336
18.6.1 软件安装.....	336
18.6.2 初识 Package.....	337
18.6.3 使用 Package 系统.....	338
第 19 章 网络上的指南针——DNS 服务器.....	341
19.1 安装 BIND.....	341
19.2 配置 named.....	341
19.2.1 设置 named.conf 文件.....	341
19.2.2 /etc/namedb/name2ip.conf 文件.....	342
19.2.3 /etc/namedb/ip2name.conf 文件.....	343
19.2.4 /etc/namedb/named.local 文件.....	343
19.2.5 /etc/namedb/named.ca 文件.....	343
19.2.6 /etc/hosts 文件.....	344
19.2.7 /etc/resolv.conf 文件.....	344
19.2.8 /etc/hosts.conf 文件.....	345
第 20 章 FTP 服务器的新星——ProFtpd.....	347
20.1 ProFtpd 快速指南.....	347
20.2 编译和安装.....	348
20.3 启动测试.....	348
20.4 proftpd.conf 文件.....	349

20.5 应用举例.....	350	第 25 章 Samba 服务器.....	375
20.5.1 隐藏 FTP 服务器版本 和信息.....	350	25.1 Samba 软件的主要组成部分.....	375
20.5.2 在 ProFtpd 环境下设置 虚拟主机.....	350	25.2 安装 Samba.....	375
第 21 章 FreeBSD 平台上的 Apache.....	351	25.3 配置 smb.conf.....	376
21.1 FreeBSD 平台上的 Apache 的 安装和启动.....	351	25.3.1 启动 Samba 的方式.....	377
21.2 设置 Apache 服务器.....	351	25.3.2 [global]设置.....	377
21.2.1 基本设置.....	352	25.3.3 [homes]个人目录共享.....	383
21.2.2 特殊配置.....	354	25.3.4 [netlogon]与[Profiles].....	383
第 22 章 邮件服务器——Qmail.....	355	25.3.5 [printers]打印机设置.....	384
22.1 简介.....	355	25.4 使用 swat 配置 Samba.....	386
22.2 所需资源.....	356	25.5 支持加密口令认证.....	387
22.3 安装过程.....	356	25.6 将 Samba 服务器加入域.....	388
22.3.1 安装 Qmail 基本包.....	357	第 26 章 俺的秘密你莫看——OpenSSH 的 安装和配置.....	389
22.3.2 安装 tcpserver 等 服务程序.....	357	26.1 OpenSSH 简介.....	389
22.3.3 安装 POP3 验证 用户程序.....	358	26.2 编译和安装.....	389
22.3.4 安装虚拟域用户 POP3 支持.....	358	26.3 配置“/etc/ssh/ssh_config” 文件.....	390
22.3.5 更改 Sendmail 为 Qmail..	358	26.4 配置“/etc/ssh/sshd_config” 文件.....	391
22.3.6 制作 Qmail 控制脚本.....	359	26.5 配置 OpenSSH.....	393
22.3.7 安装监视工具.....	359	第 27 章 FreeBSD 查漏补缺.....	395
22.3.8 Qmail 的 Web 解决方案..	360	27.1 日志问题.....	395
第 23 章 重量级的廉价数据库服务器 ——MySQL.....	363	27.2 关于 SSH 配置.....	396
23.1 MySQL 的安装.....	363	27.3 网络部分.....	397
23.2 启动和停止 MySQL.....	364	27.4 Crontab 和 at 问题.....	399
23.3 管理与使用.....	364	27.5 inetd 和 rate 限制问题.....	399
23.4 mysqladmin 公用程序的使用....	367	27.6 Securelevel 问题.....	399
第 24 章 天堑变通途——FreeBSD 上的 NFS	369	27.7 一些本地安全的提示.....	400
24.1 NFS 服务器.....	369	27.8 信息过滤问题.....	400
24.2 NFS 客户.....	370	27.9 用户资源限制问题.....	402
24.3 使用 fstab.....	371	第 28 章 管理员的反击 ——UNIX 应急响应.....	405
24.4 自动安装守护进程.....	371	28.1 应急响应的目标和任务.....	405
		28.2 应急响应的主要阶段.....	405
		28.3 初始响应.....	406
		28.4 深入调查.....	412
		28.5 应急响应分析.....	416

网络服务器安全配置详解

Linux 篇

第 1 章 UNIX 世界初探

Linux 是一个诞生于网络、成长于网络且成熟于网络的奇特的操作系统。1991 年，芬兰大学生 Linus Torvalds 萌发了开发一个“自由”的 UNIX 操作系统的想法。当年，Linux 就诞生了。为了不让这个羽翼未丰的操作系统夭折，Linus 通过 Internet 发布了自己的作品 Linux。从此一大批知名的、不知名的电脑黑客、编程人员加入到开发过程中来，使 Linux 逐渐成长起来。

Linux 一开始要求所有的源代码必须公开，并且任何人均不得从 Linux 交易中获利。然而，这种纯粹的自由软件的理想对于 Linux 的普及和发展是不利的，于是 Linux 开始转向 GPL，成为 GNU 阵营中的重要一员。

同时，Linux 作为 UNIX 家族的一员，许多特性与 UNIX 是相同的，它们之间的最大区别在于以下两点。

- UNIX 系统大多是与硬件配套的，而 Linux 则可运行在多种硬件平台上。
- UNIX 是商业软件，而 Linux 是自由软件，是免费并公开源代码的。

现在，Linux 凭借其优秀的设计、不凡的性能，加上 IBM、Intel、CA、Core、Oracle 等国际知名企业的大力支持，市场份额逐步扩大，逐渐成为主流操作系统之一。目前已经应用到以下各领域。

- 教育领域：设计先进、公开源代码这两大特性使得 Linux 成为了操作系统课的活教材。
- 网络服务器领域：稳定、健壮、系统要求低、网络功能强，这些优点使得 Linux 成为现在 Internet 服务器操作系统的首选，现已达到了 25% 的市场占有率。
- 企业 Intranet：可以用低廉的投入架设 E-mail 服务器、WWW 服务器、代理服务器、透明网关、路由器。
- 视频制作领域：著名的电影《泰坦尼克号》中的特技效果就是由 200 多台 Linux 协作完成的。

下面我们就从 UNIX 开始，进入我们的 Linux 之旅。

1.1 UNIX 简介

UNIX 于 1969 年在美国的 AT&T 贝尔实验室诞生。在过去的 30 年里经过不断锤炼，它已经成为一个在网络功能、系统安全、系统性能等各个方面都非常优秀的操作系统，至今已风行了 30 多年。现在 UNIX 已演化出不同厂家的 20 多个分支 100 多个版本，成为世界上使用最普遍的操作系统之一。

在 UNIX 发展的早期，系统的源代码是公开的，但是从 Version 7 开始，AT&T 将 UNIX 商业化，更换了许可协议，不再公开系统的源代码，从而迈出了 UNIX 商业化的第一步。

从 20 世纪 70 年代末开始，在市场上出现了不同的 UNIX 商品化版本，比较有影响的版本包括：Sun 公司的 Sun OS、Microsoft、SCO 公司的 XENIX、Interactive 公司的 UNIX386/ix 和

DEC 公司的 Ultrix。后来陆续出现的比较著名的 UNIX 系统包括：IBM 公司的 AIX、HP 公司的 HP-UX、SCO 公司的 UNIX 和 ODT，以及 SUN 公司的 Solaris 等产品。

作为 UNIX 技术的发明者和拥有者，贝尔实验室和 AT&T 公司先后发布了一系列的 UNIX 版本，包括：Edition 1（1971 年）、Edition 3（1973 年）、Edition 6（1975 年）、Edition 7（1979 年）、PWB（1979 年）和 System III（1981 年）、System V（1983 年）、SVR 2（1984 年）、SVR 3（1987 年）、SVR 4（1989 年）等版本，其中，SVR 4 作为 AT&T 和 SUN 公司联合主推的工业化版本，得到了许多重要计算机厂商的支持，成为 UNIX 工业界的主流技术。

许多厂商在此技术基础上开发出自己的商业化 UNIX 产品。到 20 世纪 90 年代初，不同的 UNIX 版本已超过 100 种，形成了 UNIX 和类 UNIX 的操作系统种类繁多的局面。为了便于引用和区分，人们就将这些操作系统合称为 U*ix、*nix……后来，UNIX 分化出两大派系：AT&T System V 和 BSD UNIX。

现在，“UNIX”已经成为 X/OPEN 组织（一个 UNIX 标准化组织）的一个商标，任何操作系统只要通过了该组织的“UNIX 兼容性测试”，就可以称做“UNIX”。由于 Linux 符合 IEEE POSIX.1 的标准，源代码与 AT&T System V 和 BSD UNIX 相兼容，并且 Linux 通过了“UNIX 兼容性测试”，也就成了“UNIX”。但从传统意义上讲，Linux 与 AT&T System V 和 BSD UNIX 没有派生关系，因此不能称为“UNIX”，它只是一个遵循 IEEE POSIX.1 标准并扩展支持所有 AT&T System V 和 BSD UNIX 特性的操作系统。

1.2 UNIX 世界的新秀——Linux

Linux 是一个诞生于网络、成长于网络且成熟于网络的奇特的操作系统。1991 年 10 月 5 日，芬兰赫尔辛基大学的学生 Linus Torvalds 发往新闻组 comp.os.minix 的一封帖子，最早向全世界宣告了 Linux 的诞生。Linux 起源于 UNIX 的变种 Minix 和公开源码。Minix 是计算机科学家 Andrew Tanenbaum（1997 年图灵奖获得者）为了方便教学和研究，以 AT&T Edition V7 为蓝本，独立开发的基于 Intel i386 平台上的一个操作系统。该系统虽然在源代码级和 Edition Version 7 兼容，但是没有引用任何 UNIX 的代码，所以它不是传统意义上的 UNIX。但是 Tanenbaum 为教学科研目的，坚持保持 Minix 代码的“纯洁性”，拒绝将 Minix 用户对其所做的工作成果加入到 Minix 中。随后，作为自由软件倡导者的 Linus 以 Minix 为基础，开始动手撰写“类 Minix”的操作系统——这就是现代 Linux 的原始模型。后来 Linus 将该自由软件献给了 GNU。GNU 是自由软件积极倡导者 Richard Stallman 于 1984 年创立的一个完全基于自由软件的软件体系。它包含一份公共许可协议（General Public License，简称 GPL），其目标是开发一个完全免费的类 UNIX 系统及其应用程序。目前，众所周知的 BIND、Perl、Apache、TCP/IP 就是自由软件的经典之作。但是，GNU 开发的名为 Hurd 的类 UNIX 系统，在开发过程中遇到了较多困难而一再滞后。自 Linus 决定把他的 Linux 交给 GNU 的时候起，Linux 就由一个人的思想变成了无数志同道合的人的一场运动。Linux 填补了 GNU 应用软件系统平台的空缺，反过来，加入 GNU 极大地推动了 Linux 的发展。Linux 诞生多年来一直停留在 Hacker 和专家的圈子里，鲜为人知。直到 1998 年，随着 Linux 自身的完善，在公开源码潮流的推动下，Linux

终于登上了大众舞台。在 IBM、Oracle、Informix、CA、Sysbase、Corel、Intel、Netscape、Dell 等许多著名计算机软硬件厂商陆续宣布对 Linux 的支持后，Linux 一下子被推上了舆论的浪尖。Linux 的所有核心代码都是由 Linux Torvald 及其他全世界最优秀的程序员完全重写的，没有 AT&T System V 或 BSD UNIX 代码，然而它却继承了 UNIX 优秀的设计思想，同时拥有世界上最大的开发群体和测试队伍，这就使 Linux 拥有干净的、健壮的并且高效的内核。在其他各种 UNIX 主要用于科学工程及高端用户的同时，由于 Linux 是基于流行的 Intel i386 及在 GNU 的通用公共许可（GPL）保护下可以免费获得的特性，使得它在经历了 Internet 中众多用户苛刻考验后成为最流行的“UNIX”。

注：什么是自由软件？

自 1984 年起，麻省理工学院开始支持“世界最后一名黑客”Richard Stallman 在软件开发团体中发起的自由软件运动，从而自由软件基金会 FSF、GPL 协议和 GNU 项目就此诞生，掀开了自由软件革命的序章。

GPL（通用公共许可协议），这是与传统商业软件许可协议“CopyRight”对立的，所以又被戏称为“CopyLeft”。GPL 保证任何人有共享和修改自由软件的自由。任何人有权取得、修改和重新发布自由软件的源代码，并且规定在不增加附加费用的条件下任何人都可以得到自由软件的源代码。同时还规定自由软件的衍生作品必须以 GPL 作为它重新发布的许可协议。

而 GNU 项目的目标是建立可自由发布的、可移植的 UNIX 类操作系统。

在 2000 年的 LinuxWorld 大会上，可以明显地感觉到：社会各界对免费发布的操作系统的支持的力度大大增强了，特别是许多硬件厂商，如 IBM、HP 和 Dell 纷纷涉足 Linux 领域，极大地促进了这种操作系统的发展。

虽然，现在纷繁复杂的多种 Linux 发行版各自为营，降低了 Linux 的整体战斗力，但业界认为，不同的发行版本最终会产生不断细分的市场，各个版本将趋向于处理某一专业领域的东西。

Linux 操作系统经历过市场风暴的洗礼之后，已经逐步创造出更多的辉煌。

1.3 Linux 的特性

Linux 是一个真正的多任务、多用户的操作系统。它充分利用了 X86 CPU 的任务切换机制，实现了真正的多任务、多用户环境，允许多个用户同时执行不同的程序，并且可以分配优先级。而这个特性只有 Windows XP 实现了，之前的 Windows NT/2000 都不是真正的多任务、多用户的操作系统。

Linux 在源代码级和一定数量的 UNIX 兼容。Linux 是遵循 IEEE POSIX.1 标准开发的，它与 AT&T System V 和 BSD UNIX 在编程接口上兼容，也就是说，UNIX 下的许多应用程序可以方便地移植到 Linux 中。

Linux 支持多达 32 种文件系统。Linux 支持常见的 FAT16、FAT32、NTFS、ISO9660 等文件系统，也支持 Minix、ext、HPFS、sysv 等许多不常见的文件系统。

Linux 是一个提供完整网络集成的操作系统。Linux 内置 TCP/IP 协议，对于 Internet/Intranet