



悦知文化
Daght Press



恒逸资讯 陈勇勋 著



刘立群 张琦 黄琨 改编
飞思科技产品研发中心 监制

Linux 网络

更安全的

防火墙 | 弱点扫描 | 入侵侦测 | Reverse Proxy | 虚拟专用网



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

[网络安全专家]

恒逸资讯 陈勇勋 著

刘立群 张琦 黄琨 改编
飞思科技产品研发中心 监制

更安全的 Linux 网络

电子工业出版社

Publishing House of Electronics Industry

北京·BEIJING

内容简介

这是一本将理论与实务完美结合的书，由网络的基本概念开始，采取以由浅入深的讲解方式，逐步引导读者进入网络安全的世界。让读者从无到有地快速向下扎根，以帮助有心跨入网络安全领域的 IT 技术人员，能够完整且正确地构建企业网络的安全屏障。

本书内容包括 Netfilter/Iptables (Linux 系统下功能最为强大且扩充能力最强的防火墙系统)；Squid Proxy (能够加速企业外连带宽，以及保护 Microsoft IIS Web Server 的重要机制)；Nessus、Snort 及 Guardian (Nessus 为 OpenSource 下功能最为完整的弱点扫描工具，可帮助我们快速且完整找出企业中有安全漏洞的服务器，进而提出问题解决的方法；Snort 则是 OpenSource 下功能最为强大的入侵检测系统，甚至可以结合 Guardian，以构成企业内部的入侵防御系统，自动将入侵者封锁于企业防火墙之外)；虚拟专用网 (企业 e 化已是当今企业生存的关键，然而网络封包的窃听已成为使用网络的一大隐忧，如何在企业 e 化与信息安全中取得平衡点？虚拟专用网可以完全解决以上所有困扰)。

本书适合系统管理与网络管理从业人员、网络安全及系统安全工作者参考学习。

本书为精诚信息股份有限公司—悦知文化授权电子工业出版社于中国大陆 (台、港、澳除外) 地区之中文简体版本。本著作物之专有出版权为精诚信息股份有限公司—悦知文化所有。该专有出版权受法律保护，任何人不得侵犯。

版权贸易合同登记号 图字：01-2009-0636

图书在版编目 (CIP) 数据

更安全的 Linux 网络 / 恒逸资讯, 陈勇勋著; 刘立群, 张琦, 黄琨改编. —北京: 电子工业出版社, 2009.3

(网络安全专家)

ISBN 978-7-121-08221-4

I. 更… II. ①恒…②陈…③刘…④张…⑤黄… III. Linux 操作系统 IV. TP316.89

中国版本图书馆 CIP 数据核字 (2009) 第 013577 号

责任编辑：杨 鹂

印 刷：北京机工印刷厂

装 订：三河市鹏成印业有限公司

出版发行：电子工业出版社

北京市海淀区万寿路 173 信箱 邮编：100036

开 本：720×1000 1/16 印张：31.5 字数：806.4 千字

印 次：2009 年 3 月第 1 次印刷

印 数：4 000 册 定价：56.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：(010) 88254888。

质量投诉请发邮件至 zlt@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：(010) 88258888。

推荐序

Linux 是一个注重实用的系统，像是练拳术一般，虽然你会练习花哨的套路，但终究是为了实战的目的。Linux 这样的系统，它不好“看”，但却扎扎实实。我常看到 IT 人员拿 Linux 在企业内部做各种不同的应用，除了常见的 Web Server、File Server 之类的应用之外，还有一个特殊的用途，那就是当做企业 IT 系统的防护罩。

目前企业的信息安全防护有个“流行”的现象，那就是在企业日常运营系统外面搭建了一层坚固异常的系统防护罩，许多企业因而会采用 Linux 做最外层或其中一层防火墙，以降低被入侵的几率。Linux 作为安全防护的机制颇为契合企业的实际用途，类似的实际功用只有 Linux 好手才知其中的诀窍。除了防火墙机制之外，企业还有常见的 Proxy 服务器，你知道可以拿 Linux 当做“反向” Proxy 服务器，反过来保护 Windows Server 的 IIS Web 服务器吗？诸如此类的实际应用，通常都是企业所需，如果你是企业内部的 IT 管理人员，建议你对于此类技术议题可以多加涉猎。

虽然 Linux 可以为企业带来许多好处，但毕竟是“马有千里之程，无人不能自往”，企业 IT 人员若不具备相关技术，给你再好的武器都派不上用场，而今即使 IT 人员愿意好好研究 Linux 相关技术，但可能也苦于参考数据的不够充足。针对 Linux 应用在企业内部网络与系统安全之议题，现在终于有了一本专书呈现在各位读者面前。本书作者 Jacky，是恒逸信息著名的 Linux 讲师之一，他授课的最大特色是会让学员觉得像是朋友般的在教授你技术知识。讲解技术的时候，逻辑条理分明，可以把复杂的 Linux 系统简单地呈现在学员面前，一

向颇受学员欢迎。以 Jacky 一贯以发扬 Linux 技术为职志的精神，由他来编写本书再恰当不过了。如果你想将 Linux 发挥在真正有用的实际场合之上，那么本书将会是你很好的参考教材。

张智凯 Richard Chang

精诚信息 \ 恒逸教育训练中心 资深处长

序

“陈老师！请问一下你有没有与 Linux 防火墙有关的著作？”

这是我在这 8 年讲师生涯中最常被学生问到的问题，但在过去 7 年之间，我都只有一个标准答案：“没有，谢谢！”主要是从来没有想过要出版任何的书籍，因为平常的工作就几乎把生活占满了，几乎腾不出任何时间来写书。

而这次之所以会有写书的念头，完全是因为看到太多关于网络信息安全的新闻，又想到自己在 Linux 的领域中这么久了，却从来没有为这个领域贡献些什么，再加上同事 John、Linda、Vivid 及悦知文化小花的怂恿，决定一次规划 3 本书成为系列，也算是为 Linux 领域贡献一点个人微薄的心力。本书是系列书籍中的第一本，至于其他两本书的出版时间，预计得等到 2009 年，因为学校教授正在追杀毕业论文阶段，还请你拭目以待！

由于本书是构建在 Linux 系统平台之上，而笔者最擅长的 Linux 平台则为 Red Hat 系统的 Linux，例如：Red Hat Enterprise Linux、Fedora Linux 及 CentOS。不过，为了让其他不同平台的 Linux 使用者也能够得以阅读，因此在编写本书时，笔者特别留意了这些问题，即使你所使用的不是 Red Hat 系列的 Linux 平台，依旧可以参考本书的内容。

陈勇勋

<http://www.bulls.idv.tw>

导读

本书是笔者结合多年来将 Linux 系统运用于网络安全的使用经验，以及 8 千多个小时授课经验所完成的著作，相信本书内容绝对可以帮助读者自学如何将 Linux 运用于网络安全。只要你能随着本书的章节一步一步地理解，一定可以很快地将 Linux 系统运用于企业网络安全的控制和管理上。

为了让读者们可以有一个实际操作的环境，笔者特地编写了“附录 A：VMware 的安装及使用”，我们可以通过 VMware 这套软件来模拟本书中 90% 以上的练习环境，可说是一套非常好的虚拟机器软件。此外，为了让使用者可以快速安装练习环境的系统，笔者将一个 Linux 系统下自动安装及配置系统的 kickstar 文件放在悦知网站（下载网址为 <http://www.delightpress.com.tw/bookSamples/SKUS00003.zip>）。如果你手边没有 Red Hat 系列的 Linux 操作系统安装光盘，可以到 <http://www.centos.org> 的网站下载 CentOS 5.x 版本的光盘 ISO 文件，至于环境的安装方法，也请你参考悦知网站下载文件内的说明文档。

以下是本书各章节的简要说明。

第 1 章：防火墙的基本概念

主要介绍防火墙的基本概念，包含防火墙的原理、防火墙的类型及防火墙的部署架构。虽然这是本书最为基础的章节，但无论如何，请你务必用心读完本章，因为后面章节中有很多概念都是构建在这个基础之上的。

第 2 章：Linux 防火墙基础篇

本章所介绍的是 Linux 防火墙 Netfilter/Iptables 的基础概念及操作方法。虽然是基础篇，但却犹如中国武术中的基本功——蹲马步，在这个章节中你将

导读

学习到 Netfilter/Iptables 系统的结构、Iptables 工具的使用方式，以及 Netfilter 的四大功能，若有任何一部分的概念不够清楚，往后章节的内容将不易吸收。

第 3 章：Netfilter 模块的匹配方式与处理方法

本章主要说明 Netfilter 的延伸模块，这是非常重要的一章。因为 Netfilter/Iptables 防火墙功能之所以强大，完全受这些扩展模块所赐，如果我们可以完整且全盘性地了解每一个模块，那么你将可以在 Linux 防火墙上执行更为复杂的连接管制动作，也可以由此让你的网络环境变得更加安全。

第 4 章：Netfilter/Iptables 的高级技巧

防火墙的性能将会影响企业连接外网的速度，在这个章节所要讨论的重点是如何有效提升防火墙的性能。因此，如果你不想花大钱更新防火墙主机的硬设备，本章内容你绝对不能错过。

此外，本章还说明构建防火墙时最令人头痛的问题——复杂通信协议穿越防火墙 NAT 的问题。如果你不想遭遇防火墙在构建完成之后却发生一堆通信协议无法使用的困境，建议你务必好好研读本章。

第 5 章：Proxy Server 的应用

这个章节主要介绍以下几个 Proxy 在企业网络中的应用，例如：如何使用 Cache Proxy 来达到节省企业连外带宽的目的；如何使用 Proxy 来进行使用者浏览网页的限制，如不得下载 EXE 文件、不得观看网页上的动画等；另外还会介绍到如何利用 Reverse Proxy 来保护 IIS Web Server。如果在你服务的公司中有使用 IIS Web Server，请千万不要错过这个单元的内容。

第 6 章：使用 Netfilter/Iptables 保护企业网络

本章以一个虚拟的企业网络来说明规划防火墙时所应该注意的事项，以及在编写防火墙规则时所需要注意的地方，此外，还包含笔者这几年来使用 Netfilter/Iptables 的私人秘笈。因此，如果你想要规划一个符合你企业需求的防火墙，本章将可引导你快速完成这项任务。

第 7 章：弱点扫描及入侵检测

你所任职的企业网络有漏洞存在吗？你担心网络因此而被入侵吗？本章将介绍三大主题，其一为如何使用弱点扫描工具，以快速且完整找出企业中已知的安全漏洞，并且快速修补这些漏洞；另外还会介绍入侵检测系统，入侵检测系统就好比网络中全年无休的保安人员，只要有任何异常的访问行为发生时，入侵检测系统会在第一时间内通知系统管理人员；最后还会介绍一个入侵检测系统的小帮手，当我们在入侵检测系统内加入这个功能之后，入侵检测系统只要检测到异常的网络访问行为，即可在第一时间内封锁试图入侵者的 IP。

第 8 章：VPN 基础篇

本章笔者将为你介绍 VPN 的完整概念、数据的加/解密原理，以及 IPSec 的完整技术概念，并通过简单的范例来引领读者快速进入 Linux IPSec 世界，最后以实例的方式来说明如何构建以 IPSec 为基础的 VPN 系统，达到加密网络上传递的数据内容。

第 9 章：VPN 实务篇

在这个章节中将介绍 IPSec 的另一个重要的协定——IKE。如果 IPSec 没有结合 IKE 机制，那么我们将无法发挥 IPSec 强大的功能，此外，本章还会介绍

导读

完整的数字证书的概念及实作。对于数字证书有兴趣或需求的读者而言，这绝对是不可错过的单元。最后，我们将数字证书与 IKE 及 IPSec 结合运用，如此将大为提升 IPSec 的安全性及可用性。

第 10 章 : VPN : L2TP Over IPSec

如果你希望在企业网络之外的公司同仁，可以在很安全的环境中，通过因特网来访问企业内部的信息，那么本章内容你绝对不能错过。因为在这个章节中，笔者将介绍如何以 L2TP Over IPSec 的机制，让一般使用者可以快速且方便地在 Windows 与 Linux 系统之间建立 L2TP 的 VPN 连接。

目录

第 1 章	防火墙的基本概念	1
	1.1 TCP/IP 的基本概念	2
	1.1.1 应用层	2
	1.1.2 传输层	4
	1.1.3 网络层	4
	1.1.4 连接层	4
	1.2 封包的传递	5
	1.3 ARP 通信协议	9
	1.4 TCP、UDP 及 Socket 的关系	11
	1.5 什么是防火墙	15
	1.6 防火墙的判别依据	17
	1.6.1 各层封包包头内的信息	17
	1.6.2 封包所承载的数据内容	19
	1.6.3 连接状态	20
	1.7 防火墙的分类	21
	1.7.1 包过滤防火墙	21
	1.7.2 应用层防火墙	22
	1.8 常见的防火墙结构	23
	1.8.1 单机防火墙	24
	1.8.2 网关式防火墙	25
	1.8.3 通透式防火墙	29
第 2 章	Linux 防火墙基础篇	31
	2.1 什么是 Kernel	32
	2.2 什么是 Netfilter	33

目录

2.3 Netfilter 与 Linux 的关系	33
2.4 Netfilter 工作的位置.....	35
2.5 Netfilter 的命令结构.....	37
2.6 Netfilter 的 Filter 机制.....	38
2.7 规则的匹配方式	42
2.8 Netfilter 与 Iptables 的关系	43
2.9 Iptables 工具的使用方法	46
2.9.1 Iptables 命令参数	46
2.9.2 Iptables 规则语法	57
2.9.3 牛刀小试：Iptables 的规则语法	66
2.10 以 Filter 机制来构建简单的单机防火墙.....	69
2.10.1 如何测试防火墙规则正确与否	72
2.10.2 解决无法在防火墙主机上对外建立连接的问题	75
2.10.3 防火墙规则数据库的管理方法	83
2.11 以 Filter 机制来构建网关式防火墙.....	85
2.12 Netfilter 的 NAT 机制.....	88
2.12.1 IP 网段的划分	89
2.12.2 Private IP	89
2.12.3 NAT	90
2.12.4 封包传递方向与 SNAT 及 DNAT 的关系	92
2.12.5 NAT 的分类	95
2.12.6 NAT 不是万能的	104
2.13 Netfilter 的 Mangle 机制.....	104
2.14 Netfilter 的 RAW 机制	108
2.15 Netfilter 的完整结构	108
2.16 实战演练	110

目录

	实战 2-1 state 模块描述下的 4 种连接状态	110
	练习 2-1 : ESTABLISHED 状态的实验	111
	练习 2-2 : RELATED 状态的实验	112
	练习 2-3 : NEW 状态的实验	113
	练习 2-4 : INVALID 状态的实验	113
	实战 2-2 以 Netfilter 构建单机防火墙	114
	实战 2-3 启动 Linux 内的 Router 机制	115
	实战 2-4 以 Netfilter 构建网关式防火墙	116
	实战 2-5 构建一对多 NAT	118
	实战 2-6 构建多对多 NAT	119
	实战 2-7 构建一对一 NAT	121
	实战 2-8 构建 NAPT	123
第 3 章	Netfilter 模块的匹配方式与处理方法	127
	3.1 匹配方式	128
	3.1.1 内建的匹配方式	128
	3.1.2 使用模块延伸出来的匹配方式	133
	3.2 处理方法	170
	3.2.1 内建的处理方法	170
	3.2.2 由模块延伸的处理方法	175
	3.3 实战演练	185
	实战 3-1 以 multiport 及 state 再加上 tcp-flags 的判别来 改写范例	185
	实战 3-2 使用 mac 模块来过滤 MAC Address	187
	实战 3-3 当有 PortScan 攻击行为发生时, 将攻击者的 IP	

目录

	锁定，使得该 IP 在 10 分钟内都不得再连接本机的任何服务	188
	实战 3-4 User Define Chain 的应用及管理	189
	实战 3-5 将 Netfilter 的 LOG 分类记录于 /var/log/netfilter 文件	191
第 4 章	Netfilter/Iptables 的高级技巧	193
	4.1 防火墙性能的最佳化	194
	4.1.1 调整防火墙规则顺序	194
	4.1.2 善用 multiport 及 iprange 模块	196
	4.1.3 善用 User Define	197
	4.2 Netfilter 连接处理能力与内存的损耗	198
	4.2.1 最大连接数量的计算	199
	4.2.2 连接追踪数量的调整	200
	4.2.3 连接追踪数量与内存的损耗	200
	4.3 使用 RAW Table	200
	4.4 简单及复杂通信协议的处理	202
	4.4.1 简单的通信协议	203
	4.4.2 复杂的通信协议	204
	4.4.3 ICMP 封包的处理原则	213
	4.4.4 在 DMZ 上使用 NAT 将面临的问题及解决方案	214
	4.4.5 常见的网络攻击手法及防护方式	217
	4.5 实战演练	237
	实战 4-1 FTP 通信协议穿越防火墙的处理	237
	实战 4-2 FTP 通信协议穿越 NAT 的处理	238

目录

第 5 章	Proxy Server 的应用	241
	5.1 什么是 Proxy Server	242
	5.2 Proxy Server 能够支持的通信协议	243
	5.3 Proxy Server 的分类	243
	5.3.1 什么是 Cache Proxy	244
	5.3.2 什么是 Reverse Proxy	245
	5.4 Proxy Server 的硬件需求	246
	5.5 安装 Squid Proxy	247
	5.6 以 Squid 构建 Cache Proxy	248
	5.6.1 Cache Proxy 的基本设置	248
	5.6.2 Cache Proxy 客户端的设置	253
	5.6.3 Cache Proxy 的高级设置	254
	5.6.4 Cache Proxy 连接访问控制	258
	5.6.5 Cache 对象的管理	260
	5.6.6 Squid Proxy 运行过程的记录文件	265
	5.6.7 Squid Proxy 名称解析的考虑	268
	5.7 Transparent Proxy	269
	5.7.1 Transparent Proxy 的工作原理	269
	5.7.2 设置 Transparent Proxy	270
	5.8 Reverse Proxy	271
	5.8.1 Web Server 的分类	271
	5.8.2 构建 Reverse Proxy	274
	5.9 实战演练	279
	实战 5-1 构建一个 Transparent Proxy	279
	实战 5-2 以 Squid Proxy 构建一个 Name Base 的 Reverse Proxy	281

目录

第 6 章	使用 Netfilter/Iptables 保护企业网络	285
	6.1 防火墙结构的选择	286
	6.2 防火墙的本机安全	288
	6.2.1 网络攻击	288
	6.2.2 系统入侵	289
	6.2.3 Inbound/Outbound 的考虑	289
	6.2.4 远程管理的安全考虑	290
	6.3 防火墙规则定义	290
	6.3.1 企业内部与因特网	291
	6.3.2 DMZ 与因特网	292
	6.3.3 企业内部与 DMZ	297
	6.4 入侵与防御的其他注意事项	297
	6.4.1 更新套件	297
	6.4.2 Syn Flooding 攻击防御	298
	6.4.3 IP 欺骗防护	300
第 7 章	弱点扫描及入侵检测	303
	7.1 什么是弱点扫描	304
	7.1.1 Nessus 弱点扫描工具	304
	7.1.2 Nessus 弱点扫描工具的操作架构	305
	7.1.3 下载及安装 Nessus 弱点扫描工具	305
	7.1.4 Nessus Client 的操作及 Report 的生成	313
	7.1.5 Nessus Server 的模块更新	319
	7.2 入侵检测系统	322
	7.2.1 网络设备的限制	322
	7.2.2 入侵检测系统的分类	324

目录

7.2.3	入侵检测系统的部署	324
7.2.4	Snort 入侵检测系统介绍	325
7.2.5	下载及安装 Snort 入侵检测系统.....	326
7.2.6	下载及安装 Snort 入侵检测系统的规则数据库.....	326
7.2.7	设置 Snort	329
7.2.8	Snort 的启动与停止	330
7.2.9	Snort 的 Alert.....	330
7.3	主动防御系统.....	331
7.3.1	取得 Guardian	331
7.3.2	安装 Guardian	332
7.3.3	设定 Guardian	332
7.3.4	Guardian 的启动与停止	334
7.4	实战演练.....	335
	实战 7-1 Nessus 工具软件的安装及操作	335
	实战 7-2 Snort 工具软件的安装及操作	336
第 8 章	VPN 基础篇	339
8.1	什么是 VPN	340
8.1.1	VPN 的原理	342
8.1.2	常见的 VPN 架构	343
8.1.3	VPN 的安全性问题	344
8.1.4	VPN 机制的优缺点	344
8.2	认识数据加 / 解密	345
8.2.1	什么是明文	346
8.2.2	什么是密文	346
8.3	数据加 / 解密的类型.....	348