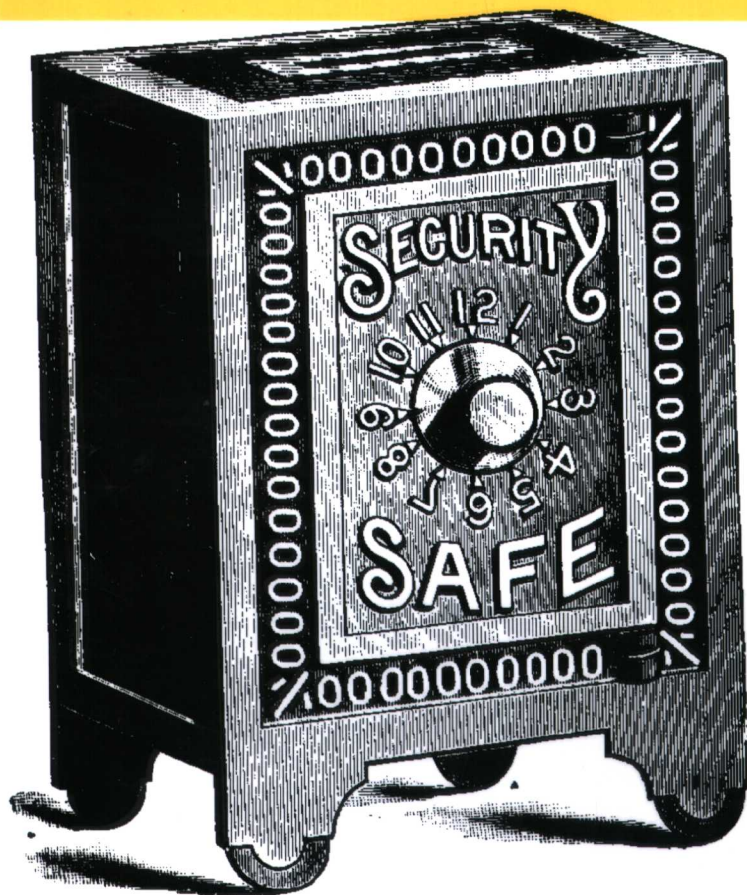


Practical Unix & Internet Security

第三版

Unix 与 Internet 安全实践指南



O'REILLY®



机械工业出版社
China Machine Press



Simson Garfinkel, Gene Spafford
& Alan Schwartz 著

王倩莉 殷海波 等译

Unix 与 Internet

安全实践指南

第三版

Simson Garfinkel, Gene Spafford

& Alan Schwartz 著

王倩莉 殷海波 等译

O'REILLY®

Beijing • Cambridge • Farnham • Köln • Paris • Sebastopol • Taipei • Tokyo

O'Reilly Media, Inc. 授权机械工业出版社出版

机械工业出版社

图书在版编目 (CIP) 数据

Unix 与 Internet 安全实践指南 (第三版) / (美) 加斐凯 (Garfinkel, S.) 等著; 王倩莉等译. - 北京: 机械工业出版社, 2005.9

书名原文: Practical Unix & Internet Security, Third Edition

ISBN 7-111-16559-4

I. U... II. ①加... ②王... III. ① Unix 操作系统 - 安全技术 ②因特网 - 安全技术

IV. ① TP316.8 ② TP393.48

中国版本图书馆 CIP 数据核字 (2005) 第 054340 号

北京市版权局著作权合同登记

图字: 01-2004-6526 号

本书法律顾问 北京市展达律师事务所

©2003 by O'Reilly Media, Inc.

Simplified Chinese Edition, jointly published by O'Reilly Media, Inc. and China Machine Press, 2004. Authorized translation of the English edition, 2003 O'Reilly Media, Inc., the owner of all rights to publish and sell the same.

All rights reserved including the rights of reproduction in whole or in part in any form.

英文原版由 O'Reilly Media, Inc. 出版 2003。

简体中文版由机械工业出版社出版 2004。英文原版的翻译得到 O'Reilly Media, Inc. 的授权。此简体中文版的出版和销售得到出版权和销售权的所有者 —— O'Reilly Media, Inc. 的许可。

版权所有、未得书面许可, 本书的任何部分和全部不得以任何形式重制。

书 名 / Unix 与 Internet 安全实践指南 (第三版)

书 号 / ISBN 7-111-16559-4

责任编辑 / 李云静

封面设计 / Edie Freedman, 张健

出版发行 / 机械工业出版社

地 址 / 北京市西城区百万庄大街 22 号 (邮政编码 100037)

经 销 / 新华书店北京发行所发行

印 刷 / 北京牛山世兴印刷厂印刷

开 本 / 787 毫米 × 1092 毫米 16 开本 52 印张

版 次 / 2005 年 9 月第 1 版 2005 年 9 月第 1 次印刷

印 数 / 0001-4000 册

定 价 / 95.00 元

(凡购本书, 如有倒页、脱页、缺页, 由本社发行部调换)

本社购书热线: 010-68326294

本书先前版本获得的赞誉

“这本书是一个非常巨大的成功，因为它在仅仅几百页的内容中包含了 Unix 和 Internet 安全的几乎所有方面。无论考虑你为本书花费的代价，还是它帮助你远离可怕的安全问题而为你节省的钱，购买本书都是一个非常好的决定。”

—— Peter G. Neumann, SRI 国际计算机科学实验室首席科学家；
ACM 计算机和公共策略委员会主席

“《Unix 与 Internet 安全实践指南》一书包含了很多实践中的脚本、技巧和警告信息，它覆盖了保证一个 Unix 系统尽可能安全的几乎全部的知识。在这个主动考虑安全问题的时代，这本书对于所有负责 Unix 系统的人都是一个必备参考。”

—— Sun World

“如果你是一个计算机安全方面的新手，应该购买本书，并每天抽出一些时间阅读它。我们阅读的进度可能很慢，但请保持一定的进度。如果你已经是一个专家，可以购买本书，并放在手边作为一个参考——每个月阅读一章，可以帮助你回忆一些已经忘记的东西。”

—— Jennifer Vesperman, linuxchix.org

“《Unix 与 Internet 安全实践指南》是一本非常畅销的图书，并且被很多人推崇。主要原因在于：其中包含了很多的信息，这些信息很容易阅读，其中的主题根据逻辑分组进行了组织。读者还会要求什么呢？”

—— Dustin Puryear, 32bitonline

“这本书及时、准确、并且是大家公认的专家所写……它包含了有关 Unix 安全的几乎所有主题。它是一本优秀的书，我推荐它作为任何系统管理员或计算机站点管理从业人员的读物。”

—— Jon Wright, Informatics

“如果你对 Linux 安全一无所知，并且只有阅读一本书的时间，你应该阅读《Unix 与 Internet 安全实践指南》这本书。”

—— Charlie Stross, Linux Format

“它是管理 TCP/IP 网络必不可少的一本书。”

—— <http://it-enquirer.com>

“很保守地说，这本书的销路非常广泛。它应用的范围太广泛了……更重要的是，它讲述了安全问题的一些基础问题，并且包含了大家常问到的一些问题——现在的软件过时后仍将存在的一些问题。”

—— Amazon.com

“充满了实践中的例子、包含了控制台命令会话的直接输出，清晰而且容易理解的图表……它是一本经典的、不可缺少的、可以信任的书。”

—— Christopher Brown-Syed, *Library and Archival Security*, Vol. 17

“《Unix 与 Internet 安全实践指南》是一本我非常推荐阅读的有关 Linux 的书。这本精心编著的书包含了有关安全的广泛问题，涵盖了很多使系统更安全的有价值的提示。”

—— Gene Wilburn, *Computer Paper*

“对于管理者来说……安全是一个非常重要的话题……非常有价值而且很重要。这本书是有关这个难题的一本好书。”

—— Peter H. Salus

“购买这本书可以节省阿司匹林。”

—— Cliff Stoll, *The Cuckoo's Egg* 以及 *Silicon Snake Oil* 书的作者

“这本书确实是来自于实践中，并且容易学会，这样，系统管理委员会始终超前于系统的攻击者一步——如果你只有阅读一本书的时间，这本书当之无愧。”

—— Kevin J. Ziese, 美国空军上校，AF 信息仓库中心对策开发部长官

“它是系统管理员书架上的一个重要组成部分。”

—— Alec Muffett, 网络安全顾问，*The Crack Program* 一书的作者

“如果你只能购买一本有关 Internet 安全的书籍，这本书当之无愧。”

—— Dan Farmer, *SATAN* 和 *COPS* 程序的作者之一

“这本书可以作为系统管理从业人员的标准桌面参考书籍。一般情况下，其有关 Unix 安全问题的广泛讲述会激发每个人对这些主题的兴趣。”

—— Paul Clark, *Trusted Information Systems*

“对于大些或者联网的系统，我推荐《Unix 与 Internet 安全实践指南》。它是一本权威的、详细的以及面向实践的书。它可以帮助你摆脱很多困扰。”

—— Richard Morin, *Unix Review*

作者简介

Simson Garfinkel 是一个新闻记者、企业家以及计算机安全的国际权威。Garfinkel 是 Sandstorm 公司的首席技术官，该公司总部在波士顿，主要开发尖端计算机安全工具。Garfinkel 还是《Technology Review Magazine》的专栏作家，并且还为止 50 个刊物撰写文章，包括《Computerworld》（计算机世界）、《Forbes》（福布斯）以及《The New York Times》（纽约时报）。他还是下列书的作者之一：《Database Nation》；《Web Security, Privacy, and Commerce》；《PGP》；《Pretty Good Privacy》以及其他 7 本书。Garfinkel 于 1988 年在哥伦比亚大学获得新闻专业的硕士学位，并且获得了 MIT 的 3 个学士学位。他目前正在 MIT 的计算机科学实验室攻读博士学位。

Gene Spafford 是一个在国际上有声望的科学家和教育家，它在信息安全、策略、计算机犯罪方面已经工作了将近 20 年。他是普度大学的教授，担任 CERIAS（世界上最先进的有关信息安全和保险的多学科学术中心）的主任。Spafford 教授和他的学生领导了很多安全领域的技术和概念的课题，包括 COPS 和 Tripwire 工具、两阶段防火墙以及易攻击的数据库。Spaf 在教学、研究、专业服务方面已经获得了大量的专业荣誉。包括：AAAS、ACM、IEEE 成员；享受国家计算机系统安全奖金；获得了 NCISSE 的 William Hugh Murray 勋章；ISSA Hall of Fame 的选举者之一；在普度大学接受 Charls Murphy 奖金。他自 2000 年就被命名为 CISSP。除了撰写有 100 多篇计算机报告和文章外，他还是《Web Security, Privacy, and Commerce》一书的作者之一，并且还是《Computer Crime: A Crimefighters Handbook》（也是 O'Reilly 出版的）一书的顾问编辑。

Alan Schwartz 是伊利诺斯大学芝加哥分校的医学教育和小儿科系的临床决策副教授。他还是《Managing Mailing Lists》的作者，也是《Stopping Spam》（也是 O'Reilly 出版的）的作者之一。他是多个 ISP 的 Unix 系统管理顾问。在他闲暇的时间，他开发并维护 PennMUSH MUD 服务器，并且同他的妻子酿造啤酒和蜂蜜酒，他们还一起抚养孩子。Alan 喜欢的刺激包括航海、用 Perl 编程、玩双桥、喝 Anchor Porter，不喜欢的是垃圾邮件和美国储藏啤酒。

封面介绍

《Unix 与 Internet 安全实践指南（第三版）》一书的封面画面是一只保险箱。保险箱的概念出现在我们的生活中已经有很长时间了。在有记录的历史开始之后，人们都在使用一些方法来确保贵重物品的安全。第一只被认为是保险箱的物理结构是由埃及人、希腊人、罗马人发明的。这些早期的保险箱是用木头制作的。在欧洲中世纪和文艺复兴时期，这些木制的保险箱开始用金属的边进行加固，某些还被加锁。第一个全金属的保险箱出现在 1820 年的法国。

Unix 与 Internet

安全实践指南

O'Reilly Media, Inc. 介绍

为了满足读者对网络 and 软件技术知识的迫切需求，世界著名计算机图书出版机构 O'Reilly Media, Inc. 授权机械工业出版社，翻译出版一批该公司久负盛名的英文经典技术专著。

O'Reilly Media, Inc. 是世界上在 UNIX、X、Internet 和其他开放系统图书领域具有领导地位的出版公司，同时是联机出版的先锋。

从最畅销的《The Whole Internet User's Guide & Catalog》（被纽约公共图书馆评为二十世纪最重要的 50 本书之一）到 GNN（最早的 Internet 门户和商业网站），再到 WebSite（第一个桌面 PC 的 Web 服务器软件），O'Reilly Media, Inc. 一直处于 Internet 发展的最前沿。

许多书店的反馈表明，O'Reilly Media, Inc. 是最稳定的计算机图书出版商——每一本书都一版再版。与大多数计算机图书出版商相比，O'Reilly Media, Inc. 具有深厚的计算机专业背景，这使得 O'Reilly Media, Inc. 形成了一个非常不同于其他出版商的出版方针。O'Reilly Media, Inc. 所有的编辑人员以前都是程序员，或者是顶尖级的技术专家。O'Reilly Media, Inc. 还有许多固定的作者群体——他们本身是相关领域的技术专家、咨询专家，而现在编写著作，O'Reilly Media, Inc. 依靠他们及时地推出图书。因为 O'Reilly Media, Inc. 紧密地与计算机业界联系着，所以 O'Reilly Media, Inc. 知道市场上真正需要什么图书。

目录

前言	1
----------	---

第一部分 计算机安全基础

第一章 概述：一些基础问题	19
---------------------	----

什么是计算机安全	21
什么是操作系统	22
什么是部署环境	23
总结	24

第二章 Unix 的历史及家族	25
-----------------------	----

Unix 的历史	26
安全以及 Unix	35
本书的作用	40
总结	41

第三章 策略和准则	42
-----------------	----

安全需求计划	43
--------------	----

风险评估	45
费用－效益分析以及最佳实践	48
策略	53
合规性审计	60
选择外包	61
“掩盖”会引起安全问题	67
总结	69

第二部分 安全地构建模块

第四章 用户、密码和认证 73

使用用户名和密码登录	73
密码的维护	80
Unix 密码系统的实现	86
网络账号和认证系统	94
可插拔认证模块 (PAM)	96
总结	98

第五章 用户、组以及超级用户 99

用户和组	99
超级用户 (root)	105
su 命令：切换用户	109
限制超级用户	117
总结	121

第六章 文件系统和安全 122

理解文件系统	122
文件的属性和权限	127
chmod：改变文件权限	135

umask	141
SUID 与 SGID	143
设备文件	152
修改文件的所有者或组	155
总结	157

第七章 密码学 158

理解密码学	158
对称密钥算法	164
公钥算法	174
消息摘要函数	180
总结	185

第八章 服务器的物理安全 186

一种被遗忘的危险	186
计算机硬件保护	189
防止窃贼	200
保护数据	204
故事：失败站点的例子	212
总结	214

第九章 人员安全 215

背景检查	216
工作中	217
离职	220
其他人员	220
总结	221

第三部分 网络和 Internet 安全

第十章 调制解调器和拨号安全	225
调制解调器：工作原理	226
调制解调器与安全	230
调制解调器与 Unix	238
调制解调器的其他安全考虑	245
总结	246
 第十一章 TCP/IP 网络	 247
网络	247
IP：网际协议	250
IP 安全	268
总结	280
 第十二章 安全 TCP 和 UDP 服务	 281
理解 Unix 的 Internet 服务器和服务	282
控制对服务器的访问	289
主要的 Unix 网络服务	302
安全地管理服务	356
综合：一个例子	365
总结	370
 第十三章 Sun RPC	 372
远程过程调用 (RPC)	372
安全 RPC (AUTH_DES)	376
总结	382
 第十四章 基于网络的认证系统	 384
Sun 公司的网络信息服务 (NIS)	385

Sun 的 NIS+	393
Kerberos	399
LDAP	407
其他网络认证系统	413
总 结	414
第十五章 网络文件系统	415
理解 NFS	416
服务器端 NFS 安全	426
客户端 NFS 安全	431
提高 NFS 安全性	432
最后的注释	439
理解 SMB	441
总 结	451
第十六章 安全编程技术	452
一个缺陷能毁坏你的一天	452
关于避免安全缺陷的提示	458
关于编写网络程序的提示	465
关于编写 SUID/SGID 程序的提示	467
使用 chroot()	469
使用密码的提示	470
产生随机数的提示	472
总 结	478
 第四部分 安全操作	
 第十七章 保持更新	481
软件管理系统	481

更新系统软件	485
总 结	490
第十八章 备份	491
为什么要建立备份	491
备份系统文件	506
备份软件	510
总 结	514
第十九章 保护账号	515
危险的账号	515
监控文件格式	526
限制登录	527
管理静止账号	528
保护 root 账号	533
一次性密码	536
传统密码的管理技术	542
入侵检测系统	552
总 结	553
第二十章 完整性管理	555
完整性的必要性	555
完整性的保护	557
检测变更	561
完整性检查工具	567
总 结	576
第二十一章 审计、日志和取证	577
Unix 日志文件工具	577
进程记账: acct/pacct 文件	599

特定程序的日志文件	601
网站日志策略的设计	605
手写的日志	608
管理日志文件	610
Unix 取证	612
总结	613

第五部分 处理安全事件

第二十二章 发现入侵..... 617

引言	617
发现入侵者	620
入侵后的清理工作	631
案例研究	643
总结	661

第二十三章 防御威胁性程序..... 662

威胁性程序：定义	663
破坏	672
开发者	673
入口	674
自我保护	675
预防攻击	686
总结	689

第二十四章 拒绝服务攻击与解决方法..... 690

攻击的类型	690
破坏性的攻击	691
超载攻击	692

网络拒绝服务攻击	708
总 结	714
第二十五章 计算机犯罪	715
入侵之后的法律选择	715
犯罪的风险	721
犯罪主题	723
总 结	725
第二十六章 你信任谁	726
能信任计算机吗	726
能信任厂商吗	730
能信任人吗	736
总 结	739
第六部分 附录	741
附录一 Unix 安全检查列表	743
附录二 Unix 进程	760
附录三 论文资源	781
附录四 电子资源	790
附录五 组织机构	803