

LINUX SERVER HACKS™

100个业界最尖端的技巧和工具

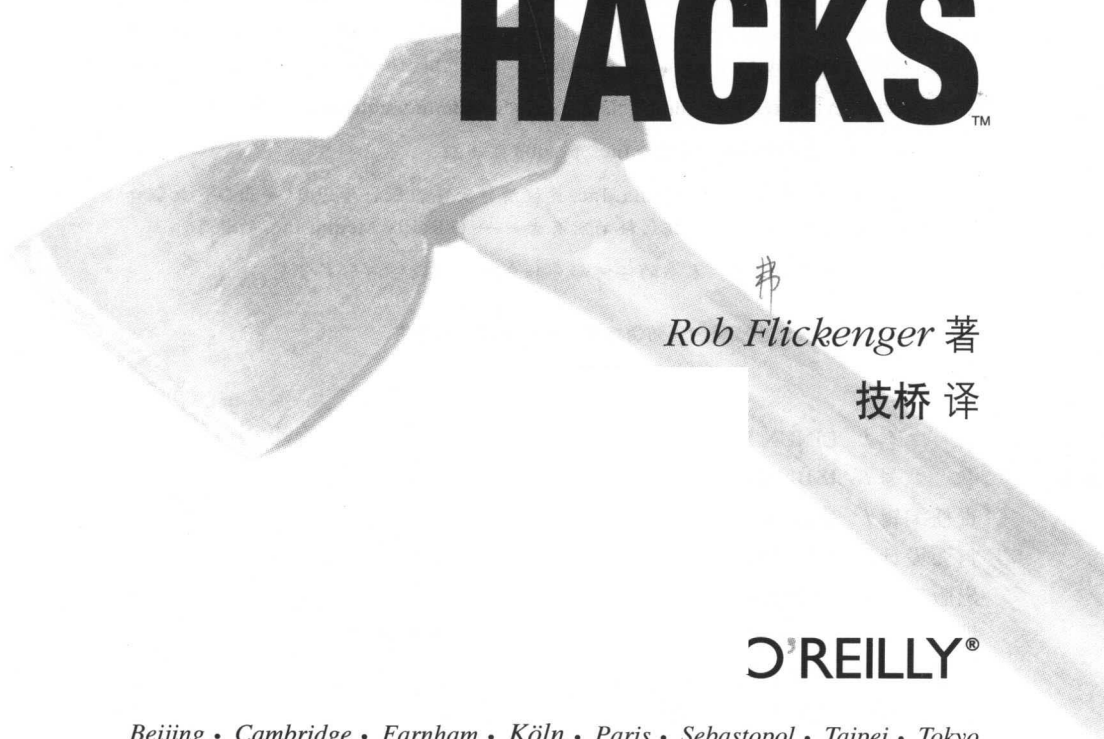


Rob Flickenger 著
技桥 译

O'REILLY®

清华大学出版社

LINUX SERVER HACKS™



弗
Rob Flickenger 著
技桥 译

O'REILLY®

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

O'Reilly Media, Inc. 授权清华大学出版社出版

清华大学出版社

图书在版编目 (CIP) 数据

LINUX SERVER HACKS/ 弗里肯格 (Flickenger, R.) 著; 技桥译. —北京: 清华大学出版社, 2004.5

书名原文: LINUX SERVER HACKS

ISBN 7-302-07169-1

I. L… II. ①弗… ②技… III. Linux 操作系统 IV. TP316.89

中国版本图书馆 CIP 数据核字 (2003) 第 077251 号

北京市版权局著作权合同登记

图字: 01-2003-3643 号

Copyright ©2003 by O'Reilly Media, Inc.

Authorized Simplified Chinese translation edition, by O'Reilly Media, Inc., is published by Tsinghua University Press, 2003. Authorized translation of the original 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.

本书之英文原版由 O'Reilly Media, Inc. 于 2003 年出版。

本中文简体翻译版由 O'Reilly Media, Inc. 授权清华大学出版社于 2003 年出版。此翻译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, 未经书面许可, 本书的任何部分和全部不得以任何形式复制。

本书封面贴有清华大学出版社激光防伪标签, 无标签者不得销售。

书 名 / LINUX SERVER HACKS

书 号 / ISBN 7-302-07169-1/TP · 5226

责任编辑 / 常晓波

封面设计 / Edie Freedman, 张健

出版发行 / 清华大学出版社 (www.tup.com.cn)

地 址 / 北京清华大学学研大厦 (邮政编码 100084)

经 销 / 各地新华书店

印 刷 / 北京四季青印刷厂

开 本 / 152 毫米 × 227 毫米 18.25 印张 240 千字

版 次 / 2004 年 5 月第 1 版 2004 年 5 月第 1 次印刷

印 数 / 0001-4000 册

定 价 / 29.00 元 (册)

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. 授权清华大学出版社, 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

如何成为一名黑客	1
----------------	---

前 言	7
-----------	---

服务器基础	15
-------------	----

1. 删除不必要的服务	18
2. 绕过控制台登录	21
3. 常用引导参数	23
4. 使用 init 命令创建可持续运行的后台程序	24
5. n>&m: 交换标准输出和标准错误	26
6. 构建复杂的命令行	28
7. 使用 xargs 处理棘手的文件	32
8. ext2/ext3 中的系统保护文件	35
9. 加速编译	37
10. 熟悉 Shell 环境	38
11. 查找并清除 setuid/setgid 二进制	42
12. 使 sudo 工作更有效	45
13. 使用 Makefile 自动执行管理任务	47
14. 强制使用新域名	50

15. 追查滥用磁盘的用户	50
16. 好玩的 /proc	52
17. 使用 procpd 符号化操控进程	56
18. 管理每个进程的系统资源	58
19. 用户离开后整理系统	60
20. 从内核中删除不必要的驱动程序	63
21. 使用大容量 RAM	65
22. hdparm:精细调整 IDE 驱动器参数	67

版本控制 71

23. RCS 入门	72
24. 在 RCS 中登出以前的修订版本	74
25. 使用 rsc2log 工具跟踪更改	75
26. CVS 入门	77
27. CVS: 登出模块	80
28. CVS: 更新工作副本	81
29. CVS: 使用标记	82
30. CVS: 更改模块	83
31. CVS: 合并文件	84
32. CVS: 添加和删除文件和目录	85
33. CVS: 分支开发	86
34. CVS: 监视和锁定文件	87
35. CVS: 保持 CVS 的安全性	88
36. CVS: 匿名仓库	89

备份 93

37. 通过 ssh 使用 tar 工具执行备份	94
38. 通过 ssh 使用 rsync 工具	96
39. 使用 Pax 命令进行存档	97
40. 备份引导扇区	104
41. 使用 rsync 工具使文件系统各部分之间保持同步	105

42. 使用 rsync 工具自动执行快照式增量备份	111
43. 使用 ISO 和 CDR/CDRW	118
44. 不创建 ISO 文件地刻录 CD	120
网络	122
45. 从任意服务器的命令行创建防火墙	123
46. 简单的 IP 伪装	126
47. iptables 的提示和技巧	127
48. 将 TCP 端口转发到任意机器上	130
49. 在 iptables 中使用自定义链	131
50. 隧道：IPIP 封装	134
51. 隧道：GRE 封装	136
52. 在 ssh 上使用 vtun 来绕过 NAT	138
53. 自动配置 vtund.conf 生成程序	145
监控	151
54. 操纵 syslog 工具	152
55. 使用 watch 工具监视作业	155
56. 是什么程序打开了那个端口	156
57. 使用 lsof 工具查看打开的文件和套接字	158
58. 使用 top 监视系统资源	161
59. 标题栏中的连续平均负载显示	163
60. 使用 ngrep 进行网络监视	164
61. 使用 nmap 工具扫描机器	167
62. 磁盘寿命分析	169
63. 廉价的 IP 接管	171
64. 运行 ntop 工具获取实时的网络状态信息	174
65. 使用 httptop 命令实时监视 Web 流量	178
SSH	186
66. 使用 ssh 客户密钥快速登录	186

67. Turbo 模式的 ssh 登录	188
68. 有效使用 ssh-Agent	190
69. 在 GUI 环境中运行 ssh-Agent	192
70. 使用 ssh 登录 X	194
71. 通过 ssh 转发端口	195
脚 本	199
72. 快速掌握 movein.sh	199
73. 使用 Perl 工具执行全局搜索和替换	202
74. 采用 bash 算法将数据分割成任意数据块	205
75. 在终端上生成彩色日志分析	207
信息服务器	210
76. 在 chroot jail 中运行 BIND	211
77. BIND 9 中的视图	214
78. 使用本地域授权建立缓存 DNS	220
79. 利用循环 DNS 分布服务器负载	222
80. 运行自己的顶级域	224
81. 使用 mtop 工具监视 MySQL 的状态	225
82. 在 MySQL 中设置复制	228
83. 从大型 MySQL 转储文件中还原单个表	232
84. 调整 MySQL 服务器	233
85. 使用带有 mysql 验证源的 proftpd 工具	235
86. 针对超级 MySQL 服务器优化 glibc、Linux 线程及内核	238
87. Apache Toolbox	241
88. 在索引中显示完整的文件名	244
89. 使用 IfDefine 工具快速更改配置	246
90. 简单的广告介绍跟踪	249
91. 使用 Apache 模拟 FTP 服务器	252
92. 旋转和压缩 Apache 服务器日志	254
93. 生成 SSL 证书和证书签发请求	256

94. 创建自己的 CA	258
95. 向客户端浏览器发布 CA 证书	261
96. 多个站点共用一个 DocumentRoot	263
97. 使用 mod_rewrite 工具根据查询字符串传递内容	266
98. 在 Apache 上使用 mod_proxy 以提高速度	268
99. 使用 Apache RewriteMap 工具分布负载	270
100. 终极宿主：使用通配符、代理和 Rewrite 宿主 大容量 Web 站点	273

如何成为一名黑客

*Jargon File*中有很多关于“黑客”(hacker)一词的定义，多数定义都说黑客拥有老练的技术，而且热衷于解决问题、突破限制。然而，如果我们只是想知道如何“变成”黑客的话，实际上只有两个相关因素。

由程序设计专家与网络奇才所构成的一个社团、一种共享文化，它的历史可以追溯到第一代分时微机及最早的 ARPAnet（阿帕网，Internet 的前身）试验。这种文化孕育出了术语“黑客”。黑客构建了因特网；黑客建立了今天的 Unix 操作系统；黑客运营着 Usenet；黑客也是使 Web 运行起来的人。如果您成为这种文化的一部分，如果您对该文化的发展做出过贡献，如果该社团中的人熟悉您而且称您为黑客，这时您就变成一个黑客了。

黑客精神并不局限于软件中的这种黑客文化。人们也以黑客态度对待其他事物，比如电子学、音乐等，实际上，我们可以在任何科学或艺术的最巅峰找到黑客的身影。软件黑客也认可其他地方的这些类似精神，也称其为“黑客”。有些人还认为：黑客本质上完全独立于其所处的特定领域。不过在本书中，我们还是将主要讨论软件黑客的技术及态度，着重分析这种能孕育出术语“黑客”的共享文化的趋势。

还有另外一群人在大声叫嚣自己也是黑客，但其实他们并不是。这些人（主要是未成年男性）闯入计算机及电话系统，他们都应该被我们一脚踢

开。真正的黑客称这些人是“解密者”(cracker)，并且不屑与之伍。真正的黑客通常都认为解密者懒惰、不负责任而且也不太聪明——能够破坏安全系统并不能让自己成为黑客，这就像即使能用铁丝开走汽车也不能让自己成为汽车工程师一样。令人遗憾的是，很多新闻记者及作家都误用“黑客”来指代解密者；这让真正的黑客非常愤怒。

最本质的差别在于：黑客创造事物，而解密者破坏事物。

如果您想成为黑客，请继续阅读本书。如果您只想成为解密者，请去阅读 alt.2600 新闻组，然后准备在监狱中呆上 5 到 10 年之后，才会发现自己并非想象中的那么聪明。我对解密者想说的话只有这么多。

黑客的态度

黑客解决问题、构建事物，他们崇尚自由与自愿的相互帮助。要想让人们把自己看成黑客，我们必须也显示出具备了这种态度。除了显示出具备这种态度之外，我们还必须确实深信这种态度。

然而，如果认为只要培养出黑客态度后就能取得黑客文化圈的认可，那就大错特错了。让自己也变成深信所有这些的人对我们来说是很重要的——这能帮助我们学习，让我们才思敏捷。就像所有创造性的艺术一样，要想成为大师，最有效的途径就是模仿那些大师的精神——不仅仅是智力上的，还包括情绪上的。

或许我们可以借助下面这首现代禅诗来阐述这层意思。

大师是怎样炼成的：

寻找大师，

模仿大师，

跟随大师，

洞察大师，

成为大师。

如果我们想要成为黑客，也要一直重复下述过程，直到坚信不移。

1. 世界上有很多有待解决的有趣问题

成为黑客当然很有趣，不过这种有趣需要极大的努力。这些努力就构成了动力。成功运动员的动力来自于一种身体上的满足，他们身体力行，不断超越自己的体能极限。与此类似，要成为黑客也要有一种最基本的冲动——冲动于问题的解决、冲动于技术的日益成熟、冲动于这种智力训练。

如果不是天生就能感受这种冲动的人，那么为了成为黑客，我们也必须要成为这样的人。否则就会发现有很多东西（如性、钱及社会认可等）会分散、泯灭掉我们成为黑客的热情。

我们还必须培养起对自己学习能力的信心——甚至即使自己对所需解决的问题一无所知，也要有这样的信心。即使我们只能解决问题的一小部分，但却能从中学习，这样所学的知识将很快能解决问题的下一部分，最终我们将能解决全部问题。

2. 任何问题都没有必要重复解决

创造性的脑力是一种无价但有限的资源。现在还有很多有趣的新问题等待解决，我们不应该把这些脑力用于闭门造车上。

行为举止要像一个黑客，我们必须相信其他黑客的思考时间都是非常珍贵的——因此，可以说道义上要求我们共享信息、解决问题、公开解决方案，这样其他黑客就可以去解决“新”问题，而不用老是重新研究老问题。

尽管公开所有创造性成果的黑客能赢得其他黑客的尊敬，但我们不要认为自己有义务必须这样做。黑客的价值同样也体现于出售自己的成果，这样黑客们才能有饭吃、有房子住、有计算机用。黑客技术最好用于养家糊口，甚至发家致富，但这么做的时候不要忘记自己对你的艺术及你的黑客同伴的忠诚。

3. 厌倦与苦干都是大忌

黑客（泛指一些有创造力的人）从来不会厌倦也不会苦干那些愚蠢的重复性工作，因为这么做只会表明他们没有去做那些只有自己能做的事情，即解决新问题。这种浪费会伤害到所有人。因此，厌倦与苦干不仅是令人郁闷的事，事实上还是我们的一大忌讳。

要想从行动举止上都像一个黑客，我们就必须坚信这一点：要尽可能地自动化处理那些烦人的琐事。不仅仅是为自己，也是为了所有其他人（特别是其他的黑客）。

不过有一个很明显的例外。人们有时会看到黑客们也在做一些重复性的、令人厌倦的工作——就像在洗脑。黑客们这么做是为了获取一种技能，或者为了取得某种特定的经验。不过这是出于无奈——任何有脑子的人都不应该强迫自己从事所厌倦的工作。

4. 自由至上

黑客本质上是反权威的。任何能命令我们的人都可以让我们停止解决感兴趣的问题，而且权威的一般思路通常都只会给出一些不可理喻的理由。因此，我们要时刻准备着与权威主义作斗争，以免扼杀我们这些黑客。

这并非说要挑战所有权威。黑客可能会接受某种权威，因为这样所取得的东西比听从命令所花费的时间更重要。不过这种交易很有限且有意识地进行；权威们所期望的那种人格投降并不在内。

权威们热衷于审查与保密。并且，他们不信任自愿合作与信息共享——他们只喜欢自己能控制的那种“合作”。因此要想让自己的行为像一个黑客，我们就必须本能地厌恶审查、保密、强行管制、欺骗责任人等行为。而且我们也必须乐于遵守这一信条。

5. 态度并不能代替能力

要想成为黑客，我们必须培养起这些态度。但只有态度并不能让我们成

为黑客，就像只有态度并不能让我们成为运动健将和摇滚歌星一样。要成为黑客，需要聪明才智、实践经验、奉献精神以及刻苦工作。

因此，我们还要具备怀疑态度，但同时要尊重每一种能力。黑客们不会把时间浪费在做秀上面，但他们看重能力：特别是黑客的能力，不过无论在哪个方面，只要有能力就值得肯定。少数人才能掌握的命令技能尤其重要，而那些思维敏锐、灵活且精炼的命令技能则是最好的能力。

如果我们能尊重能力，那么也会乐于培养自己的能力——刻苦的工作与奉献精神将会导演一场狂热的演出，而不是一件苦差事。这种态度对成为一名黑客是特别重要的。

文章全文请参见在线 Web 页 <http://www.tuxedo.org/~esr/faqs/hacker-howto.html>，也可以参见 *Cathedral and the Bazaar* (O'Reilly 公司出版) 一书的附录。

— Eric S.Raymond

Eric S.Raymond 是 *New Hacker's Dictionary* 一书（根据 Jargon File 编写）及著名的 *Cathedral and the Bazaar* 一文（这相当于 OpenSource 运动的宣言）的作者。下面的内容摘自他 1996 年的一篇文章 *What is a hacker*。Raymond 认为黑客是致力于解决有趣问题的天才，这个思想正是 O'Reilly Hacks 系列书籍的基调。

前言

黑客因为爱其他的人才做黑客
并不是为了钱而做黑客。

— /usr/games/fortune

hack（黑客）这个词有很多含义。“出色的黑客技术”能最有效地利用现有环境，使用手头上的所有资源。而“拙劣的黑客技术”则使用最晦涩的方式（也是最不容易让人理解的方式）来进入环境，不过，很多“出色的黑客技术”最初看起来也有点愚蠢。

黑客技术的效率一般可以用其解决特殊技术问题的能力来衡量，其效率与问题解决过程中所投入的人力成反比。有些黑客技术还可以进一步升级，而有些黑客技术已经稳定了。运行时间最长、最广为接受的黑客技术就成了标准，从这个标准可以发明出更多的技术。出现了下一种更好的黑客技术之后，现在的黑客技术就会退出历史舞台。

黑客揭示了抽象代码与设计者丰富复杂思维之间的接口，同时还揭示了人类需求中清楚而粗俗的一面。有时候，黑客会很丑恶，它的存在仅仅是因为有点痒需要挠挠。从工程角度看，黑客完全就是DIY（Do It Yourself，自己动手）的意思：没有人会理解为什么黑客会比那些最初就被迫来解决问题的人要好。热衷于解决问题的人们会认为某一种黑客很丑恶，因此，他们多数都义无反顾地来促成更好的黑客技术——即破解那些黑客技术，这也正是我们鼓励本书读者要做的。

最后，即使是功能最强的服务器，即使服务器上拥有目前最多的RAM并

运行着最快的（大部分情况下是空闲的）操作系统，但仍然只是一种解决短期问题的权宜之计，最终人们还会需要更好、更快、更便宜的方案。

上面这些伪哲学理论会将您引向何方？我们希望这些背景知识能让您大致了解一下本书的思路，本书正是按照这种思路来组织这些问题的解决方案集合，因此本书称作 *Linux Server Hacks*。其中，有些解决方案短小而简单，而另外一些则非常复杂。所有这些黑客方案都是为解决特定的技术问题而设计的，设计者当然不希望这些方案没有“挠到痒痒”就被扔了。我们希望其中一些方案能够直接挠到某几个“痒处”（不论是 Linux 服务器管理员新手，还是有经验的 Linux 服务器管理员，都会有一些比较挠头的问题）。

本书组织结构

合格的系统管理员必须是一个万事通。要想成为真正有效率的管理人员，要求我们能处理系统出现的每个问题，从电源问题直至挂起问题。为了能够帮助读者尽快理解这些问题，本书列举了一些节省时间且新颖的日常管理任务。

- “服务器基础”首先讲述了系统管理中所遇到的一些最常见的任务：控制引导进程；有效运用命令行；自动化常见任务；监视（并调节）系统资源的使用；调节 Linux 内核的各种参数以提高系统的运行效率。本章并不是对系统管理的介绍，而只是讲述一些非常有效但鲜为人知的技术，即使是有经验的系统管理员也可能会忽视这些技术。
- “版本控制”一章简要地讲述了两种基本的版本控制系统（即 RCS 和 CVS）的使用方式。能够快速调用配置文件、源代码、文档等的任何版本是省时省力的关键。太多的专业管理员都缺乏基本的版本控制知识（喜欢执行一些看似必然实则不受支持的 *.old* 或 *.orig* 备份）。这一章将唤醒那些管理员，让他们行动起来，同时本章还给出了中肯而扼要的命令及说明。