科爱传播
KE'AI COMMUNICATIONS

21世纪信息安全大系

Linux网络安全实践

Mohan Krishnamurthy Madwachar, Eric S. Seagren, Raven Alder
Aaron W. Bayles, Josh Burke, Skip Carter, Eli Faskha 著
邱硕 孙海滨 刘乙璇 译

How to Cheat at Securing Linux

科学出版社

How to Cheat at Securing Linux

Linux 网络安全实践

Mohan Krishnamurthy Madwachar
Eric S. Seagren
Raven Alder
Aaron W. Bayles
Josh Burke
Skip Carter
Eli Faskha

著

邱 硕 孙海滨 刘乙璇 译

科学出版社

北京

图字：01-2008-2326 号

ISBN 13：978-1-59749-207-2

图书在版编目(CIP)数据

Linux 网络安全实践/(巴林) 马德瓦查尔 (Madwachar, M. K.), (美) 西格伦 (Seagren, E. S), (美) 奥尔德 (Alder, R.) 著；邱硕，孙海滨，刘乙璇译. —北京：科学出版社，2009

ISBN 978-7-03-023636-4

Ⅰ. L… Ⅱ. ①马…②西…③奥…④邱…⑤孙…⑥刘… Ⅲ. Linux 操作系统-安全技术 Ⅳ. TP316.89

中国版本图书馆 CIP 数据核字 (2009) 第 014950 号

责任编辑：田慎鹏 霍志国/责任校对：郑金红
责任印制：钱玉芬/封面设计：耕者设计工作室

科学出版社出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

骏走印刷厂印刷
科学出版社发行 各地新华书店经销

*

2009 年 4 月第 一 版 开本：787×1092 1/16
2009 年 4 月第一次印刷 印张：19 1/2
印数：1—4 000 字数：438 000

定价：49.00 元

(如有印装质量问题，我社负责调换〈环伟〉)

贡献作者

Mohan Krishnamurthy Madwachar（OPSA，SPST） 是巴林 Almoayed Group 公司网络安全主管。他是公司工程部的核心成员，也是网络安全部的重要创始人。Mohan 具有极强的网络、安全及培训背景。他曾在 Schlumberger Omnes 公司和 Secure Network Solutions India 公司任职，在大规模复杂网络方面具有丰富经验，是一位安全工程专家。

Mohan 是 IT 工业标准、系统厂商认证、网络及安全界的领袖，IEEE 和 PMI 成员。Mohan 把本书献给他的兄弟 Anand、Anand 的妻子 Preethi. Anand 和他们可爱的女儿 Janani。Mohan 还是 Syngress 出版的《Designing and Building Enterprise DMZs》（ISBN：1597491004）和《Configuring Juniper Networks NetScreen and SSG Firewalls》（ISBN：1597491187）两本书的合作作者。Mohan 也为报纸写作，还作为主题专家为优秀的内容提供商撰写技术文章。

Eric S. Seagren（CISA，CISSP-ISSAP，SCNP，CCNA，CNE-4，MCP+I，MCSE-NT）在计算机行业拥有 10 年的经验，近 8 年就职于一家排行财富前 100 名的金融服务业公司。Eric 的计算机职业生涯始于一家休斯敦的公司，他在那里使用 Novell 服务器并处理网络故障。由于曾有金融领域的经验，他负责的事务越来越多，包括管理服务器、灾难恢复以及业务协调、解决千年虫问题、网络漏洞评估和风险管理。近年来，Eric 主要从事 IT 构架和风险分析的工作，对网络的安全性、可扩展性和冗余性进行设计和评估。

Eric 作为特约作者或技术编辑参加编写了多本图书，如《Hardening Network Security》（McGraw-Hill 出版）、《Hardening Network Infrastructure》（McGraw-Hill 出版）、《Hacking Exposed：Cisco Networks》（McGraw-Hill 出版）、《Configuring Check Point NGX VPN-1/FireWall-1》（Syngress 出版）、《Firewall Fundamentals》（Cisco Press 出版）、《Designing and Building Enterprise DMZs》（Syngress 出版）。Eric 还获得了美国 Toastmasters 的 CTM。

Aaron W. Bayles 是休斯敦 Sentigy 公司的高级安全顾问。他对 Sentigy 的客户的企业网进行渗透测试、漏洞分析和风险评估。Aaron 在 INFOSEC 具有 9 年以上的工作经验，尤其精通无线安全、渗透测试和事件响应。他曾作为 SAIC 公司的高级安全工程师，在维吉尼亚和得克萨斯州工作过。Aaron 是 Syngress 出版的《InfoSec Career Hacking，Sell your Skillz，Not Your Soul》一书的第一作者。

Aaron 为美国财政部和国土安全部中多个部门提供了 INFOSEC 支持和渗透测试，如财政部的 Financial Management Service and Securities and Exchange Commission 部门和国土安全部的 U. S. Customs and Border Protection 部门。Aaron 取得计算机科学学士学位后在 Sam Houston 州立大学从事嵌入式 Linux 程序开发。他也是一位 CISSP。

Raven Alder 是 IOActive 公司的高级安全工程师，IOActive 公司致力于网络安全的设计与实现。Raven 重视纵深防御，精通企业级安全的可扩展性问题。她能够设计大规模防火墙和 IDS 系统，然后进行漏洞分析和渗透测试，以确保系统安全稳定。Raven 利用业余时间在 LinuxChix.org 上讲授网络安全课程，还研究开源软件的密码漏洞。Raven 住在西雅图。她对《Nessus Network Auditing》（Syngress 出版，ISBN：1-931836-08-6）一书也有贡献。

Everett F.（Skip）Carter 博士 是 Taygeta Network Security Services 公司（Taygeta Scientific Inc. 公司的分公司）总裁。Taygeta Scientific Inc. 在科学计算、智能仪器、特殊数据分析领域提供咨询。Taygeta Network Security Services 公司则在防火墙和 IDS 的实时管理和监控、被动流量分析审计、外部安全审查、取证和事件调查方面提供服务。

Skip 拥有哈佛大学应用物理专业硕士和博士学位，麻省理工学院物理和地球物理两个学士学位。他是 American Society for Industrial Security（ASIS）成员，Syngress 出版的《Hack Proofing XML》（ISBN：1-931836-50-7）的特约作者。他发表了大量科技论文，是 Forth Dimensions 杂志的前专栏作家，也为 Dr. Dobbs Journal 和 Computer Language 撰写文章。

Josh Burke（CISSP） 是西雅图的独立信息安全顾问。过去 7 年中，他曾在技术、财经和媒体部门从事网络、系统和安全的工作。毕业于华盛顿大学商学院，Josh 在处理信息安全事务时重视技术与业务需求之间的平衡。他在公司推行一种包容的、积极的安全哲学，鼓励大家讨论采用安全策略的原由和好处，而不是一味灌输禁令。

Josh 是开源安全软件专家，精通 Snort、Ethereal 和 Nessus 等软件。他愿意研究并改进 DNS（Domain Name System）和 NTP（Network Time Protocol）的安全性和适应性。他也喜欢阅读数学和关于密码历史的书籍，但是读得越多，就发现自己了解得越少。

Eli Faskha（Security＋，Check Point Certified Master Architect，CCSI，CCSE，CCSE＋，MCP） Eli 是巴拿马 Soluciones Seguras 公司的创始人和总裁。公司专攻网络安全，是 Check Point 的金牌合作伙伴和诺基亚授权合作伙伴。Eli 曾是 Syngress 出版的《Configuring Check Point NGX VPN-1/Firewall-1》（ISBN：1597490318）一书的助理技术编辑，也是 Syngress 出版的《Building DMZs for the Enterprise》（ISBN：1597491004）的特约作者。Eli 是该地区最有经验的 Check Point 认证安全顾问和诺基亚顾问，曾用英语和西班牙语指导过来自 20 多个国家的客户。1993 年他毕业于宾夕法尼亚州的 Wharton 学院和 Moore 工程学院，1995 年获得乔治敦大学 MBA 学位。他有 8 年以上互联网开发经验，1999—2000 年间致力于巴拿马最大的 Internet portal 网站的开发。2001 年起管理了 Verisign 公司的一个分部，同时开始运作自己的公司。Eli 在当地媒体上发表了一些文章，对建设巴拿马互联网的贡献得到了公众的认可。

译 者 序

本书是一本非常实用的关于Linux系统网络安全配置的指导性读物。它涉及了几乎所有常见网络安全问题。内容上，理论与实践相结合，着重描述了各领域技术背景以及相应开源免费软件的使用。结构上，各章由浅入深依次展开，但又可以各自独立，一般不必以前文为基础。本书一大特点是，作者往往列举出多个类似的技术或功能相同的软件，进行横向比较，然后选择性地进行详述，这样帮助读者既获得广博的知识面，又能够精通一两项常用技能。

本书的主要目标读者为Linux系统管理员、安全管理员，以帮助他们选择采用哪种系统和技术，并提供了全面且深入的操作方法。Linux系统的使用者也有必要学习系统安全知识，了解网络安全特点，以在使用时多加注意。信息化建设相关人员、学生、网络安全研究人员以及广大对网络安全技术和网络安全软件感兴趣的人们，也可以从中获取有益的前沿信息和技术。

本书第1，2，3，6，9，10章由邱硕翻译，第5，7章由孙海滨翻译，第4，8章由刘乙璇翻译，第11章由刘鹏友情翻译。全书由邱硕统一修改并定稿。特别感谢博士生刘笑寒、李安南和孙国栋，他们为本书的译稿做出了重要的贡献。

原书语言流畅，内容严谨，具有极强的实用性和可操作性。译者力求反映原书的风貌和特点，但由于时间以及水平有限，不当和疏漏之处在所难免，恳请广大读者批评指正。我们的电子邮箱是qiushawn@yahoo.com。

译者

2009年2月　北京

目　录

Chapter 1

第 1 章
开源软件的商业应用案例

本章主要内容：

- 使用免费方案的花费
- 使用免费方案节省的经费
- 免费与商业解决方案的比较
- “推销”免费方案

√ 小结

√ 快速解决方案

√ 常见问题

引言

也许你在寻求一种廉价的方法来解决系统安全问题，并且想了解更多的免费软件。本书将指导你学习一些最佳解决方案，它们使得 Red Hat Linux 更加安全。在有些环境下，不管是否有一个完善的计划，提议和实施任何类型的安全措施都会引发问题。本章给予必要的帮助和支持，以实现一个节省开支的方案。

人们常常扮演两种角色：一，实施安全性改进，期望上级接受方案；二，你是一位决策者，需要了解某个“免费”的解决方案实际含义，不论你是哪种人，本章都会找到解决办法。本章讨论了使用免费软件时的隐性开销，揭示开销的来源。本章还谈到这样的事实：在多数情况下，一个免费软件与一个商业产品，在统一标准下进行公平的比较是不切实际的。掌握了上述信息，你就能够在提出方案时占得先机，也能使自己的观点更有商业说服力。

使用免费方案的花费

在安全问题解决方案的案例中，几乎没有什么东西是终生免费的。可能一个方案本身无需付费，但方案的实现却是有开销的，而这一点很容易被忽略。在多数案例中，选择哪个解决方案取决于其安全性的需求，如果没有可用的免费方案，就不得不使用商业化的工具。然而幸运的是，世界上有很多高质量的免费方案。本书后面章节里也有这方面的内容，目的是对解决方案给予不同深度的描述。如果没有足够的知识和调研就轻率地开始实施一种免费的方案，这可能会比使用商业方案花费更多的经费。

培训费用

当采用一种免费的解决方案时，培训费用是最大的开支之一。其一是直接的培训费用（如送某人去参加课堂学习）。当需要针对免费软件进行培训时，几乎别无选择。多数情况下，培训课程并不具有很强的针对性（例如，恐怕找不到 netfilter 防火墙的课程），然而可以参加一些间接的培训，如一般性的 Linux 使用或者系统管理课程。

另一项支出是材料费（如书本）。除现有资料外，可能有些领域需要专门的知识。例如部署一个 Snort 入侵检测系统（IDS），而现有资料只涉及了如何安装 Snort，所以需要购买关于这个软件的其他图书。

还有一种培训代价，就是职员在培训期间无法工作。这期间他没有贡献，而你在支付资源，所以说员工离开工作岗位也是一种损失。即使员工在工作岗位自学培训内容，也同样是一种消耗。

购买硬件

一个安全设备应该是一种不需要依赖计算机的设施，只能用于设计的用途，然而所有的解决方案都需要在计算机平台上运行。幸好，它们对平台的要求很低，可以使用旧的 PC 机，而且有些软件的安装也比较简便。但也有其他的情况，一些软件（如嗅探

器、入侵检测系统（IDSes），或网络流量报告工具）的物理位置会导致系统不安全。如果系统无法申请到足够的资源，则不能保证机器上所有的程序都能够有效运行（如 Snort 入侵检测系统的日志记录会快速消耗磁盘空间，几乎不给其他程序留下资源）。

如果没有可用的老式系统，可以从网络零售商那里购买一些廉价的旧机器。低端 PC 机的很大一部分成本来自操作系统，而很多零售商提供装有 Linux 的廉价机器或者根本没有安装操作系统的机器。这样，你就能够低价买到相对较新的机器，然后自行安装操作系统。在运行安全工具和提供用户工作站时，这是一种可行的选择。

咨询费用

必须仔细斟酌和平衡支出项目。如果培训得不够，最终就要聘请咨询顾问了。所以，实施、配置、维修一个免费的防火墙的开销可能很大，甚至超过购买一个防火墙产品。小型的商业防火墙售价大约 5 百/500 美元，而一个免费方案有可能很快让你花费更多。

即使这样，如果有必要，也别吝惜聘请咨询顾问。和使用有版权的方案相比，如果一名高级顾问为你配置免费解决方案，并且通过最佳的操作来实现该方案，还是相当划算的。同时，咨询顾问也可以扮演培训师的角色，你可观察他如何工作，而且可以提出问题，请教为什么必须这样或那样做。这样，既请到技术全面、经验丰富的人实施了解决方案，同时又能给内部人员提供培训和指导。

如果你有过不得不聘请咨询顾问的经历，可能发现这并非总是物有所值。有时，他们的技术没有想象得那么出色。与咨询公司进行沟通是非常关键的，最好能让他们确切了解你的需求。一个好的咨询顾问可以化繁为简。

警　告

削减咨询费用预算时，一定要谨慎。我见过为了降低成本最后却开销更大的案例。在几乎所有的情况下，尽快聘请咨询顾问是首选的行动方针，对于长期运作也具有最佳的成本效益。如果遇到一名你所器重的有才干的咨询顾问，每月进行例行咨询也是值得投资的。

隐性开销

免费解决方案的全部开销是什么呢？没有经验的人的答案是：电能消耗。我有一个只用于打印机服务的 Windows 98 系统，每月电费大约 7 美元。购买一个专用的打印服务器只需要 30 美元，而且不耗电。我只需要积攒 5 个月的电费就可以购买一台专用的打印服务器。在 Pentium II 上运行 Windows 98 无需进行技术性投资，然而运行时的耗电使得成本效益没有达到最优。有的安全装置是作为商业设备推出的，而有些则是免费的（例如，小型的、低成本的防火墙比一些厂商的标准桌面 PC 机大大减少了耗电量）。因而，电费成本也有不同。查看电费账单，精确算出某个设备的耗电量。

另一个需要考虑的事项是散热（Heating）、通风（Ventilation）和空调设施（Air Conditioning）的费用（HVAC）。HVAC 主要是指控制温度。新增的计算机引入新的

热源，导致空调开销的增加。这里同样也要考虑耗电的问题。如果设备没有包含降温装置，那么不可避免地要增设 HVAC 设施。安装高效散热设备的地方，往往会比一个普通的工作站发热要少。老式计算机和较新的计算机也有不同，一台较新的计算机高负荷运转时，耗电更多，需要大量散热，但通常包含比老式系统更高级的节能特性。

还有一项不动产开销。一台淘汰的全尺寸塔式计算机，比起新型的小型商业设备，要占用大得多的空间。也许你现在有一个足够大的房间，而逐渐地，当这个房间越来越拥挤的时候，空间就成问题了。一套 KVM（Keyboard、Video、Mouse）设备省下的空间比它的售价更有意义。随着服务器结构日益紧凑，对空气流通的方式和降温措施的要求将越来越高，同时，对系统中物理器件的操作和维护也更加困难。

如果考虑技术支持人员可能不熟悉新采用的免费解决方案，操作效率低也是一种损耗。当技术人员对新防火墙执行工作时，要比在所熟悉的防火墙上工作时花费更多的时间。这种低效拖延了完成任务的时间。特别是期间若出现损耗或交易被终止的情况，将导致损失利润甚至失去整桩生意。因此，在制定计划或者进行其他业务时，一定要考虑这种拖延。

免费的解决方案通常是由小型组织或者个人开发的。这些方案在它们所在的领域里往往非常优秀，但是可能并不为人所知。当实施免费解决方案的人离开以后，维持这个系统就成了问题。例如，使用一个广为所知 PIX 防火墙，定位某个资源可能并不困难。然而，如果需要别人接管一个复杂的免费方案，找到合适的人选都是十分困难的。当问题很晚才暴露出来的时候，就会发现，这种延迟也是一种隐性开销。此时，你不得不付给咨询顾问额外的报酬，或者为低效造成的其他损失买单。

使用免费方案节省的经费

本节讨论使用免费解决方案是如何节省经费的。首要的一项显而易见：这个产品本身不用花钱，然而除此之外，还有其他的益处。下文详细描述了采用免费解决方案的种种好处。通过评估预期的节省和支出费用，你就能对采用免费解决方案所产生的效果有一个更实用、更精确的理解。

节省购买成本

使用免费软件所节省的最大一项单独开销是购买成本。防火墙是最好的例子，一个 Linksys 或 Netgear 的小型防火墙，大约要 2000～5000 美元。这样的防火墙耗电小、支持端口转发（Port Forwarding）、能够执行网络地址转换（Network Address Translation，NAT）、能作为 DHCP（Dynamic Host Configuration Protocol）服务器，又是一个基于状态的包过滤（Stateful Packet Filtering）防火墙。假设在 Linux 上运行 netfilter 免费防火墙，可能会比购买一个 Linksys 防火墙开销更大，这种开销用在员工安装这个系统的工时上。只要能买得起，商业解决方案往往更容易实现，防火墙是最典型的代表之一。

即使购买产品，也可以有节约成本的办法。有些类型的产品，特别是如入侵检测系统（IDSes）、网络分析和报告工具，还有商业虚拟专用网络（Virtual Private Network，