TURING 图灵系统与网络管理技术丛书

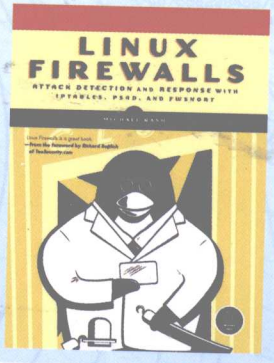
no starch press

Linux Firewalls
Attack Detection and Response with iptables, psad, and fwsnort

Linux防火墙

[美] Michael Rash 著
陈健 译

- Amazon五星盛誉图书
- 世界级安全技术专家力作
- 防火墙技术和入侵检测技术的完美结合



人民邮电出版社
POSTS & TELECOM PRESS

TURING 图灵系统与网络管理技术丛书

Linux Firewalls
Attack Detection and Response with iptables, psad, and fwsnort

Linux防火墙

[美] Michael Rash 著
陈健 译

人民邮电出版社
北京

图书在版编目（CIP）数据

Linux 防火墙 /（美）拉什（Rash, M.）著；陈健译 .
—北京：人民邮电出版社，2009.6
（图灵系统与网络管理技术丛书）
书名原文：Linux Firewalls：Attack Detection and Response with iptables, psad, and fwsnort
ISBN 978-7-115-20580-3

Ⅰ. L… Ⅱ. ①拉…②陈… Ⅲ. ①Linux 操作系统②计算机网络－防火墙 Ⅳ. TP316.89 TP393.08

中国版本图书馆CIP数据核字（2009）第037938号

内 容 提 要

本书创造性地将防火墙技术和入侵检测技术相结合，充分展示开源软件的威力。书中全面阐述了 iptables 防火墙，并详细讨论了如何应用 psad、fwsnort、fwknop 3 个开源软件最大限度地发挥 iptables 检测和防御攻击的效力。大量真实例子以及源代码更有助于读者理解安全防御的原理、技术和实际操作。

本书讲解清晰且实用性很强，适合 Linux 系统管理员、网络安全专业技术人员以及广大计算机安全爱好者阅读。

图灵系统与网络管理技术丛书

Linux防火墙

◆ 著 [美] Michael Rash
译 陈 健
责任编辑 傅志红
执行编辑 印星星

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街14号
邮编 100061 电子函件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
北京隆昌伟业印刷有限公司印刷

◆ 开本：800×1000 1/16
印张：16.75
字数：396千字 2009年 6 月第 1 版
印数：1－3 000册 2009年 6 月北京第 1 次印刷
著作权合同登记号 图字：01-2008-3299号

ISBN 978-7-115-20580-3/TP

定价：49.00元

读者服务热线：(010)51095186 印装质量热线：(010)67129223
反盗版热线：(010)67171154

版 权 声 明

译 者 序

诚如Richard Bejtlich在序言中所说，本书是一本好书，这也是我在翻译完本书后的第一感受。与目前市面上其他介绍防火墙或入侵检测技术的书籍相比，本书最大的特点是实用性。书中既没有空洞地大谈理论而让普通读者望而却步，也没有只谈论安全软件的配置和使用而让读者感觉味同嚼蜡，不知所以。作者以其简练、清晰的笔法将安全防御的原理、技术和实际的操作娓娓道来，即使读者只是一个网络安全的门外汉，也能通过阅读本书而迅速地成长为一位安全专家。更重要的是，本书介绍的所有安全软件都是开源的，Michael Rash在书中创造性地使用开源软件将防火墙技术和入侵检测技术相结合，向我们展示了开源软件的威力。而且因为书中介绍的3个软件psad、fwsnort和fwknop的作者就是Michael Rash本人，所以书中对这些软件的介绍无疑是最为权威和准确的。

我相信本书对各种层次的读者都将有所帮助。如果你是网络安全员，那么本书将向你展示Linux系统在这方面所能实现的毫不逊色于商业软件的强大功能；如果你是网络安全软件开发人员，那么本书将给你提供许多灵感和启发，书中处处闪烁着作者在网络安全防御技术方面的真知灼见；如果你只是普通的Linux用户，通过阅读本书，你也会惊叹于开源软件iptables的无限可扩展性和其强大的威力，并对网络安全技术及其发展趋势有深刻的理解。

我在翻译过程中对原书中的一些明显错误进行了更正，对书中介绍的软件，也参照其最新版本对改动之处添加了译者注。但限于水平，译文中错误之处在所难免，真诚希望读者能提出指正意见，以便在本书重印时作出修订。

最后感谢人民邮电出版社图灵公司的编辑，没有他们始终如一的鼓励和督促，本书是很难翻译完成的。

陈　健

2008年秋于南京大学

序　言

当听到防火墙这个术语时，大多数人会想到在OSI参考模型的网络层和传输层检查网络流量并做出允许通过或过滤决定的产品。其实从产品角度来说，目前存在着几十种类型的防火墙产品，它们是根据所检查的数据源（例如，网络流量、主机进程或系统调用）以及检查的深度来分门别类的。几乎任何检查通信流量、并决定是允许它通过还是将它过滤的设备，都可以视为一个防火墙产品。

代理防火墙的发明者和第一个商业防火墙产品的实现者Marcus Ranum在20世纪90年代中期给出了防火墙的一个定义，他说："防火墙是对因特网安全策略的实现。"[①]这是一个非常好的定义，因为这个定义与产品无关、永恒而且现实。它既适用于那时由William R. Cheswick和Steven M. Bellovin所著的最早的一本防火墙图书《防火墙与互联网安全》（*Firewalls and Internet Security*，Addison-Wesley Professional，1994），也同样适用你现在正在阅读的这本书。

依照Ranum定义的精神，防火墙还可以被视为是一个策略执行系统。检查网络流量并做出允许通过或过滤决定的设备可以称为网络策略执行系统；检查主机活动并做出允许通过或过滤决定的设备可以称为主机策略执行系统。不管是哪种情况，强调策略执行将引导我们重点关注防火墙的正确角色，即防火墙是一个实现策略而不是仅仅"阻止坏事物"的设备。

说到"坏事物"，我们不禁要问：在如今的企业中，防火墙是否还能起作用。正确配置的传统网络防火墙产品只允许管理员认可的互联网协议、IP地址、TCP/UDP端口以及ICMP的类型和代码通过。在现代的攻击环境中，这种程度的防御是远远不够的。虽然说对攻击渠道的限制对于限制目的地进出路径是十分必要的，但是至少最近十年来，网络层和传输层过滤始终是一种非常不充分的防攻击对策。

2007年，最有效的入侵客户端的方式是引诱用户激活恶意的可执行文件、发送给用户包含恶意内容的链接或攻击用户经常使用的另一个客户端组件。在许多情况下，攻击并不依赖于理应修复的漏洞或加固的配置。相反，攻击者可以利用如今浏览Web网页越来越需要的富媒体平台（如JavaScript和Flash）中的弱点来实施攻击。

---

① 《计算机安全杂志》（*Computer Security Journal*）Vol. XI，No. 1，Spring 1995（http://www.spirit.com/CSI/Papers/hownot.htm）。

2007年，最有效的入侵服务器的方式是绕开操作系统而去利用应用程序的漏洞。Web应用程序在服务器领域占据了统治地位，它们更有可能遭受到针对其架构和设计上的缺陷实施的攻击，而不是针对能用补丁修复的漏洞所实施的攻击。在20世纪90年代末，人们热衷于通过改变用户购物车中物品的价格来演示一个不安全的Web应用程序。拜Ajax所赐，购物车在十年后运行在了客户端，同时价格仍然能被改变，而情况也因此变得更糟。

所有这一切似乎使得防火墙产品的前景变得相当黯淡。许多防火墙产品为了适应新的发展需要，集成了对OSI参考模型的应用层进行深度数据包检查或操作的能力。其他一些防火墙产品则成为*入侵防御系统*，它们通过利用巧妙的营销术语将自己与市场上其他的产品相区分。在这个客户端攻击肆虐和利用Web应用程序漏洞的时代，防火墙产品，特别是开源的产品，是否还能占据一席之地呢？

答案是肯定的——而且你正在阅读其中一种解决方案。Michael Rash是创造性利用网络技术防御攻击的先行者。安全研究和开发领域似乎正逐渐被各种攻击工具和技术所统治，我们只需快速浏览一下某次拉斯维加斯黑客大会上的发言者名单就能清楚这一点。与这一趋势相对抗，Michael一直在发明并改进保护资产免受攻击的方法。在看过黑客大会所呈现的网络黑暗面后，几乎我们所有人都将返回到现实的工作中来保护我们的企业。谢谢这本书让我们又有了一套程序和方法集让工作变得更轻松。

在阅读本书的初稿时，我发现了几点作者想要阐述的主题。首先，以主机为中心的防御正在变得越来越重要，因为设备都是独立并暴露在因特网中的。这种演变的一个极端例子就是IPv6的引入，它的部署将还原最初因特网“端到端”的特性。当然，*端到端*也可以被看作为是*攻击者到受害者*，所以我们需要一种能实现主机自我保护的方式。本书将告诉你如何使用基于主机的防火墙和工具来实现主机的自我保护。

其次，尽管主机必须增强自身的防御能力，但仅仅围绕主机展开防御是不够的。一旦主机被入侵，它就无法再继续进行自我防御了。在入侵系统之后，入侵者通常会关闭主机防火墙、防病毒软件和其他防护机制。因此，在可能的情况下，我们仍然需要使用网络过滤设备。一个被入侵的端主机只能使用网络防火墙允许的通信渠道，这至少限制了入侵者可以享有的自由空间。本书也将告诉你如何使用网络设备来保护主机。

最后，我们必须找到富有创意的方法来保护我们的资产，并深入理解攻击场景。如果想限制对敏感服务的访问，那么与端口碰撞相比，单数据包授权是一个巨大的进步。对日志和流量进行可视化显示将有助于分析员检测出原本难以察觉的事件。通过阅读本书，你可能会发现其他人（甚至包括作者）都没有想到的方法来充分利用你的防御基础设施。

我很高兴以一个书评人和技术书作者的身份来总结这些想法。自2000年至2007年年中，我阅

读了近250本技术书籍，写了不少书评，我自己也出了几本书，因此，我自信能够判断出什么叫一本好书。《Linux防火墙》就是这样一本好书。我是一个FreeBSD用户，但在看过这本书后，我已在考虑在某些场合使用Linux了！Michael的书写得异常清晰、井井有条、简洁明了，操作性强。你只需按照书中例子里说明的过程，就可以实现作者介绍的所有技术。通过阅读本书，你不仅会熟悉安全工具和技术的使用方法，还将领悟到作者那敏锐的防御观。

世界上大多数数字安全专业人员都非常关注防御技术，而攻击技术通常只有坏人、警察和军队才用。我非常欢迎像《Linux防火墙》这样的图书出现，它为大众带来真正的防御工具和技术，而且这些工具和技术只需付出最低的成本和努力就可以被消化和部署。祝本书好运——我们都需要它。

Richard Bejtlich
TaoSecurity主席兼CEO
通用电气公司应急响应部主管
于弗吉尼亚州Manassas Park

前　言

网络攻击看来正在日益得势。几乎每一天都会听说发生了新的针对软件漏洞的攻击，要么就是出现了一个更有效的散布垃圾邮件的方法（我的收件箱可以证明这一点），或者就是某公司或政府机构的敏感个人数据被窃这种轰动一时的事件。实现安全计算是一个永恒的挑战。我们并不缺乏挫败狡猾的黑帽黑客的技术，但他们仍然在不断地成功入侵一个又一个系统和网络。

每一类安全问题都有对应的开源解决方案或专有的解决方案。在网络入侵检测系统和网络访问控制设备（防火墙、过滤路由器等）方面尤其如此。防火墙技术的一种发展趋势是将来自入侵检测范畴的应用层检测技术与过滤网络流量的能力相结合，一些防火墙早就已经开始这么做了。本书的目的就是向读者显示Linux系统上的iptables防火墙可以充分把握这一趋势，特别是当它与一些旨在从入侵检测角度充分利用iptables的软件相结合时更是如此。

我希望本书在已出版的相关著作中是独一无二的。市面上已有一些讨论Linux防火墙各个方面的优秀书籍，但就我所知，还没有一本书是专门讨论通过iptables及其提供的数据来检测（并在某些情况下挫败）攻击的。市面上还有许多介绍入侵检测的书籍，但没有一本书侧重于介绍如何真正地使用防火墙技术来辅助入侵检测过程。本书讨论的则是如何将这两种技术进行结合。

我会在书中用大量的篇幅来介绍3个开源软件项目，它们旨在最大限度地发挥iptables的效力以检测和防御攻击。这3个项目是：

- psad——iptables日志分析程序和积极回应工具；
- fwsnort——将Snort规则转换为等价的iptables规则的脚本；
- fwknop——iptables的单数据包授权（SPA）的一个实现。

所有这些项目都是按照GNU公共许可证（GPL）的规定以开源软件的形式发布的，它们都可以从http://www.cipherdyne.org网站上下载。

为什么要使用 iptables 来检测攻击

ROSENCRANTZ：我是说，你们到底做什么呢？

PLAYER：平时，我们或多或少做些自己份内的事情。在舞台上，我们按剧情要求进行表演。

其实每一个出口也可以是一个入口，如果你能这么看待的话，那事情就圆满了。

——汤姆·斯托帕德《君臣人子小命呜呼》

如果你运行的是Linux操作系统，那么很有可能遇到过iptables防火墙。我这么说是有充分理由的，因为iptables提供了一个有效的手段来控制谁可以并如何通过网络连接到Linux系统。在因特网这个浩瀚自由的网络中，攻击可以来自全球的任何一个角落——虽然作恶之人可能就在附近。如果运行一个联网的Linux主机，系统时时刻刻都将冒着被攻击和入侵的危险。

部署一个严格的iptables过滤策略是维护一个强大安全实体的第一步。即使你的Linux系统所连接的网络已受到上游的另一个防火墙或其他过滤设备的保护，但该上游设备总是有可能无法提供足够的保护。比如这类设备可能配置不当，也可能遇到bug或其他故障，或不具备防御某类攻击的能力。所以在有可能的情况下实现一定程度的冗余是非常重要的，在每个Linux系统（服务器和桌面机）上运行iptables所带来的安全利益要大于因此所付出的额外管理开销。换句话说，在Linux基础设施中部署并维护iptables所付出的成本肯定要小于系统被入侵或有价值的数据丢失所带来的损失。

本书的主要目标是向读者显示如何从检测和回应网络攻击的角度来最大限度地利用iptables。采用iptables策略对用户访问Linux系统上服务的行为进行限制是完成这个目标的第一步，但你将很快看到还需要做更多的事情。

专用的网络入侵检测系统怎么样

对入侵进行检测的工作通常是留给专门的系统来处理的，它们就是为这个目的设计的，并且它们对本地网络有着广泛全面的了解。本书并不主张改变这个策略。专用的网络入侵检测系统（IDS）作为负责保护网络安全的基础设施的一部分，其地位是不可替代的。此外，IDS可以收集到的原始数据包中的数据是一个宝贵的数据源。每当安全分析员需要搞清楚在攻击或系统入侵中究竟发生了什么时，原始数据包中的数据是至关重要的，可用于顺藤摸瓜，而来自IDS的事件则可以指明调查的方向。如果没有IDS对可疑活动发出警告，分析员可能完全不会想到系统遭受到了攻击。

本书主张的是将iptables作为现有入侵检测基础设施的一个补充。虽然iptables主要用于对网络流量加以策略限制，而不是检测网络攻击，但它所提供的强大功能使其能够模拟一些传统上只属于入侵检测范畴的重要功能。例如，iptables的日志格式提供了网络层和传输层首部中几乎所有字段（包括IP和TCP选项）的详细数据，而且iptables的字符串匹配功能可以针对应用层数据执行字节序列的匹配。这类功能对于检测入侵企图是至关重要的。

入侵检测系统通常都是被动设备，它们没有被配置为针对可能怀有恶意的网络流量自动采取任何惩罚行动。一般而言，这么做是有充分理由的，因为这可以避免误将正常的流量看作怀有恶意的流量（即误报）。但也有一些IDS可以被部署为线内模式，当系统以这种方式部署时，通常就

称为网络入侵防御系统（IPS）[①]。因为iptables是一个防火墙，所以它总是以线内模式运行的，这使得它可以在许多攻击造成重大损失之前将它们过滤掉。出于保障网络的基本连通性和网络性能的考虑，许多机构一直在犹豫是否在它们的网络基础设施中部署一个线内模式的IPS，但在某些情况下，基于应用层检查条件来过滤流量又是非常有用的。在Linux系统上，iptables可以通过将IDS签名转换进iptables策略以阻止网络攻击的方式来提供基本的IPS功能。

纵深防御

纵深防御是一个从军事上借用的原则，它常在计算机安全领域中应用。它规定我们必须在一个任意系统的各个层次都考虑到受攻击的可能性，攻击可能来自于计算机网络或一个实际的军事设施等各个方面。没有任何事情可以确保攻击绝不会发生。而且，一些攻击可能会成功地入侵或破坏一个系统的某些组件。因此，在系统中的各个层次部署多级防御机制是非常重要的，这样一来，当攻击入侵了一个安全设备时，另一个设备仍能正常工作以阻止它造成更多的损害。

在网络安全领域，最优秀的开源入侵检测系统是Snort，许多商业厂商也生产了优秀的防火墙和其他过滤设备。但如果你的基础设施中运行的是Linux系统，那么你需要考虑的真正问题是仅仅依靠这些安全机制来保护关键资产是否明智。纵深防御原则表明iptables可以作为对现有安全基础设施的一个重要补充。

先决条件

本书假设读者比较熟悉TCP/IP网络概念和Linux系统管理。如果读者对OSI参考模型、主要的网络层和传输层协议（IPv4、ICMP、TCP和UDP）以及DNS和HTTP应用层协议也比较了解的话，会对理解本书的内容很有帮助。虽然书中会经常提到OSI参考模型中的各层，但主要讨论的是其中的网络层、传输层和应用层（分别对应的是第3、4和7层），会话层和表示层在书中没有提及，物理层和数据链路层只是简略提到（有关第2层过滤的详细信息可以在http://ebtables.sourceforge.net上找到）。本书对网络层、传输层和应用层的涵盖强调了攻击可能在上述每一层中发生——我们假设读者对这些层的结构和功能都比较熟悉。虽然我们并没有专门讨论无线协议和IPv6，但书中的许多例子都同样适用于这些协议。

如果读者具备一些基本的编程实践（尤其是Perl和C编程语言），那么对理解本书的内容也将是有益的，书中的代码示例一般都会被细分和解释。书中有些地方还会显示由tcpdump以太网嗅探器捕获到的原始数据包中的数据，因此若用过以太网嗅探器（如tcpdump或Wireshark）也将有助于你阅读本书。除了上面提到的这些内容以外，我们并不要求读者必须具备计算机安全、网络入侵检测或防火墙概念的知识才能阅读本书。

① 尽管IPS有着这样一个冠冕堂皇的名字和供应商永无休止的营销炒作，但如果网络入侵防御系统没有一种方法来检测攻击，那么它就什么都不是——而检测机制就来自IDS领域。网络IPS通常只是增加了一些额外的设施来处理线内流量并回应攻击。

最后，因为本书主要讨论的是对网络攻击的检测和回应，所以书中一般不讨论主机级的安全问题，如通过删除编译器来加固运行iptables的系统、大量削减用户账号、打上最新的安全补丁，等等。Bastille Linux项目（见http://www.bastille-linux.org）提供了很好的主机安全方面的信息。对于真正的核心安全员来说，美国国家安全局的SELinux发行版（见http://www.nsa.gov/selinux）在这方面是个很好的榜样，它从系统中最重要的组件——内核本身开始增强系统的安全性。

技术参考

下面列出的都是一些优秀的技术参考书籍，它们为本书所介绍的内容提供了更多的技术细节。

- 《构建Internet防火墙》第2版（*Building Internet Firewalls*，Elizabeth D. Zwicky，Simon Cooper和D. Brent Chapman著，O'Reilly公司2000年出版）；
- 《计算机网络》第4版（*Computer Networks*，Andrew S. Tannenbaum著，Prentice Hall公司，2002年出版）；
- 《防火墙与Internet安全：击退狡猾的黑客》第2版（*Firewalls and Internet Security*：*Repelling the Wily Hacker*，William R. Cheswick，Steven M. Bellovin和Aviel D. Rubin著，Addison-Wesley公司2003年出版）；
- 《Linux系统安全》第2版（*Linux System Security*，Scott Mann和Ellen L. Mitchell著，Pearson Education公司2002年出版）；
- 《Perl语言编程》第3版（*Programming Perl*，Larry Wall，Tom Christiansen和Jon Orwant著，O'Reilly公司2000年出版）；
- 《网络安全监控之道：超越入侵检测》（*The Tao of Network Security Monitoring*：*Beyond Intrusion Detection*，Richard Bejtlich著，Addison-Wesley公司2004年出版）；
- 《TCP/IP指南》（*The TCP/IP Guide*，Charles M. Kozierok著，中文版人民邮电出版社2008年出版）；
- 《TCP/IP详解，卷1：协议》（*TCP/IP Illustrated*，*Volume 1*：*The Protocols*，W. Richard Stevens著Addison-Wesley公司1994年出版）。

有关网站

本书中包含一些示例脚本、iptables策略和命令、网络攻击案例和相关的数据包捕获。所有这些材料都可以在本书的网站http://www.cipherdyne.org/LinuxFirewalls上下载。拥有这样一份电子副本是自己修改并试验本书中的概念和代码的最佳方式。该网站还提供了psad、fwsnort和fwknop项目的使用示例和文档，以及使你能够查看每个项目源代码的Trac接口（http://trac.edgewall.com）。每个项目的源代码都被小心地保存在一个Subversion版本库（http://subversion.tigris.org）中，使我们可以很容易地看出代码是如何从一个版本改进到下一个版本的。最后，读者还可以在该网站上找到一些有趣的iptables日志数据的图形表示。

如果在阅读本书时有任何问题，你还可能在本书的网站上找到答案，当然也可以直接问我，我的电子邮件地址是mbr@cipherdyne.org。

每章摘要

你在阅读本书的过程中将接触到许多内容，本节提供各章的简要概述，让你提前了解将要学习的内容。

第 1 章：iptables 使用简介

这一章介绍如何使用iptables进行数据包过滤，包括内核编译的细节和iptables管理。这一章还提供了一个默认的策略和网络图，本书的其余章节都将参考这个策略和网络图。运行默认策略的Linux主机作为局域网（LAN）的防火墙，针对这个系统的攻击将在后续章节中说明。

第 2 章：网络层的攻击与防御

这一章介绍了网络层的攻击类型，以及我们的应对办法。我将向读者介绍iptables日志格式，并强调可以从iptables日志中收集到的网络层信息。

第 3 章：传输层的攻击与防御

传输层是使用端口扫描和端口扫射实现服务器侦查的领域，这一章将研究这些方法的内部机理。iptables的日志格式非常适合于表示传输层首部信息，这些信息可用于检测各种类型的攻击。

第 4 章：应用层的攻击与防御

如今的大多数攻击都是在利用位于TCP/IP协议簇顶端的日益复杂的应用层的漏洞。这一章说明了iptables可以检测到的各类应用层攻击，并介绍了iptables的字符串匹配扩展。

第 5 章：端口扫描攻击检测程序 psad 简介

这一章讨论psad的安装和配置，并展示为什么倾听iptables日志叙述的故事是那么地重要。

第 6 章：psad 运作：检测可疑流量

psad提供了许多功能，旨在最大限度地发挥iptables日志信息的作用。psad可以检测各种可疑活动（从端口扫描到后门探测）并通过详细的电子邮件和syslog警报来报告这些活动。

第 7 章：psad 高级主题：从签名匹配到操作系统指纹识别

这一章介绍psad的高级功能，包括集成的被动式操作系统指纹识别、通过数据包首部实现

Snort签名检测、详细的状态信息和DShield报告。这一章显示了iptables日志信息在提供安全数据方面所能发挥的巨大作用。

第 8 章：使用 psad 实现积极回应

如果对入侵检测的讨论没有提及自动回应攻击，那么这样的讨论就是不完整的。psad提供的回应功能是建立在整洁的接口之上的，它使得psad与第三方软件的集成变得更加容易，这一章包括了一个psad与Swatch项目集成的例子。

第 9 章：转换 Snort 规则为 iptables 规则

Snort IDS向IDS社区显示了基于网络攻击的检测方法，因此在iptables中充分利用Snort签名语言是合乎逻辑的。因为iptables提供了丰富的日志记录格式和检查应用层数据的能力，所以有相当数量的Snort签名都可以转换为iptables规则。

第 10 章：部署 fwsnort

将Snort签名转换为iptables规则的繁琐任务由fwsnort项目来自动完成。这一章将告诉你它是如何完成的。部署fwsnort将赋予你的iptables策略以入侵检测的能力。

第 11 章：结合 psad 与 fwsnort

由fwsnort生成的日志信息可以被psad识别并分析，从而通过电子邮件更好地进行报告（电子邮件中包括了集成的whois、反向DNS查询以及被动式操作系统指纹识别）。这一章代表了攻击检测的最高点和iptables可以做到的减缓策略。

第 12 章：端口碰撞与单数据包授权

被动授权对于保持网络服务的安全正变得越来越重要。通过使用这类技术，零日攻击的破坏范围将大大受到限制，但并不是所有的被动授权模型都适用于关键部署。这一章将对比两种被动授权机制：端口碰撞和单数据包授权（SPA）。

第 13 章：fwknop 简介

目前可以使用的SPA实现很少，fwknop是其中开发最活跃并受到广泛支持的SPA实现。这一章将讲述如何安装fwknop并将fwknop与iptables结合起来以维护默认丢弃的iptables策略，该策略将阻止所有未经验证和授权而企图连接到你的SSH守护进程的行为。

第 14 章：可视化 iptables 日志

最后一章介绍iptables日志数据的图形化表示。图形可以快速地展现网络通信中的变化趋势，揭示可能的系统入侵活动，通过将psad与AfterGlow项目相结合，可以洞悉iptables日志数据中原

本难以发现的关联。

附录 A：攻击伪造

剖析Snort签名规则集，然后使用伪造的源地址构造一个匹配这些签名的数据包是极其容易的。附录A讨论了一个Perl脚本示例（与fwsnort项目一起发布），该脚本就是用来做这件事情的。

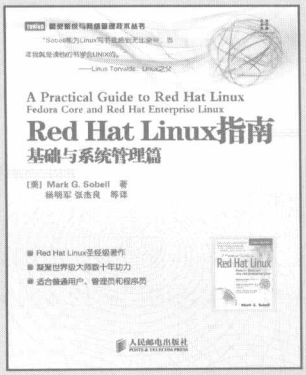
附录 B：一个完整的 fwsnort 脚本

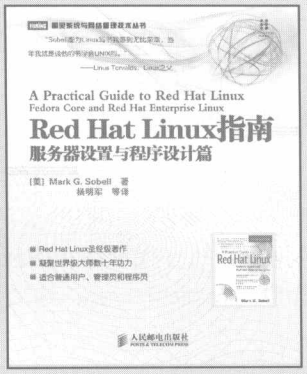
fwsnort项目创建一个shell脚本自动执行iptables命令，必须执行这些命令才能创建一个能够检测应用层攻击的iptables策略。附录B包含了一个由fwsnort生成的fwsnort.sh脚本的完整示例。

本书采用的是一种高度实用的写法。理解概念的最好方法莫过于研究实例，而研究源代码或仔细检查数据包跟踪总是理解计算机工作原理的最佳方式。希望读者通过阅读本书，可以掌握使用iptables来检测并处理网络攻击的实用知识。再次重申，我欢迎读者向我提问，我的电子邮件地址是mbr@cipherdyne.org。

致谢

本书在撰写并出版的每一步中都得到了很多人的帮助。我要特别感谢No Starch出版社的工作人员所付出的努力。William Pollock、Bonnie Granat、Megan Dunchak和Christina Samuell都投入了许多时间对本书的书稿进行专业编辑，从而使本书能以更高的质量呈现给读者。我要对Pablo Neira Ayuso说，谢谢你一直以来为协助开发Netfilter和iptables所付出的努力，谢谢你帮助完成了本书的技术编辑工作。Ron Gula（Tenable网络安全公司的CTO）和Raffael Marty（Splunk公司的首席安全战略决策者）都对本书贡献了建设性的批评意见，并在本书出版前就极力推荐。我还要感谢Richard Bejtlich（TaoSecurity主席兼CEO）为本书写了这么好的序言。“Richard，你的著作一直在激励着我。”我还要特别感谢我的父亲James、母亲Billie和我的兄弟Brian，谢谢他们一直以来对我的鼓励。最后，我要衷心谢谢我的妻子Katie，没有她的帮助，本书是不可能完成的。





Linux之父强烈推荐的圣经级著作

原书名：A Practical Guide to Red Hat Linux: Fedora Core and Red Hat Enterprise Linux ,3rd Edition
作者名：（美）Mark G. Sobell

内容简介

本书是知名Linux 专家Mark G.Sobell 的经典著作。中文版将原书分为了两卷，上卷为基础与系统管理，下卷为服务器设置与程序设计。上卷共分四大部分，全面讲解了Red Hat Linux 。第一部分主要介绍Red Hat Linux 系统（包括Fedora Core 和Red Hat Enterprise Linux）的安装。第二部分详细讲述Red Hat Linux 的登录、GUI 、实用工具、文件系统和shell 等内容。第三部分深入详细地讨论Red Hat Linux 系统的工作机制。第四部分讨论系统管理。本书最后还有一个500 多条的术语表。此外，书中每章最后都附有练习题，可以帮助读者巩固所学内容。

下卷分为两大部分，第一部分深入讨论了服务器的安装和运行以及服务器与客户端的连接，介绍了各种最流行的Linux服务器。第二部分讲解Linux编程开发相关技术，涵盖了各种编程工具，讲述了如何调试C程序和如何使用共享库，并介绍了流行的Bash Shell下面的脚本编程技术。此外，书中每章最后都附有练习题，可以帮助读者巩固所学内容。

本书赞誉

“Sobell 能为 Linux 写书我感到无比荣幸，当年我就是读他的书学会 UNIX 的。”

——Linus Torvalds，Linux 之父

“我从事教育行业，发现 Sobell 所著的这本书非常适合企业中需要掌握 Linux 的人们，对他们大有裨益。Sobell 写书思路非常清晰。他精心创作每章的内容，直至章末练习题，而这些练习题都是用户或者管理员在日常工作中会碰到的现实问题。信息技术和信息系统专业的学生将会发现这本书是一本极有价值的学习参考书。本书信息量极大，而 Sobell 对这些信息出色地驾驭，合理地安排，作者紧扣主题，从不绕弯子说题外话。对于那些在网络环境中管理 Linux 系统或者运行 Linux 服务器的人来说，这是一本必备的书。另外，我也要向那些刚转到 Linux 平台的有经验的计算机用户极力推荐本书。”

——Mary Norbury 科罗拉多大学丹佛校区 Barbara Davis 中心 IT 主管

“感谢你的辛勤劳动和你所著的书。能够像本书这样帮助人们成为各类工作站的有效管理员的图书太少了。我们（在俄罗斯）希望你能够继续给我们带来有关理解 Linux/UNIX 系统方面的新图书。”

——Anton Petukhov 律师、作家兼记者

“一本非常优秀的参考书！既适合 Linux 集群系统管理员，又适合那些打算安装最新稳定版 Linux 的 PC 用户。不要因为本书吓人的重量而犹豫。Sobell 的这本书包罗万象，满足你做系统管理工作的全部需求。”

——Wes Boudville 发明家

“本书是我所见过的概述 Linux 操作系统最好的一本书……无论读者的背景如何，是传统的 UNIX 用户，还是新的 Linux 发烧友，甚至是 Windows 用户，本书对他们都应该是非常有帮助的，也是非常好理解的。书中每个主题都讲述得清晰而完整，不要求读者有多少背景知识……作为参考书本书极其有用，它有 70 页的术语表，并且还有非常实用的索引。本书经过了精心组织，读者可以集中精力学习简单的任务，待准备妥当再去学习更高级内容。”

——Cam Marshall Marshall 信息服务公司 Front Range UNIX 用户小组 [FRUUG] 成员

目　录