

<<Linux防火墙>>

图书基本信息

书名：<<Linux防火墙>>

13位ISBN编号：9787115205803

10位ISBN编号：7115205809

出版时间：2009-04

出版时间：人民邮电出版社

作者：Michael Rash

页数：247

字数：396000

译者：陈健

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<Linux防火墙>>

前言

诚如Richard Beitlich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。

<<Linux防火墙>>

内容概要

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。

<<Linux防火墙>>

作者简介

Michael Rash世界级的安全技术专家，以防火墙、入侵检测系统等方面的造诣享誉安全界。他是psad, fwknop, and fwsnort等著名开源安全软件的开发者的安全架构师。

除本书外，他还与人合撰了Snort 2.1 Intrusion Detection和Intrusion Prevent

<<Linux防火墙>>

书籍目录

第1章 iptables使用简介 1.1 iptables 1.2 使用iptables进行包过滤 1.3 安装iptables 1.4 内核配置 1.5 安全性和最小化编译 1.6 内核编译和安装 1.7 安装iptables用户层二进制文件 1.8 默认iptables策略 1.9 本章总结 第2章 网络层的攻击与防御 2.1 使用iptables记录网络层首部信息 2.2 网络层攻击的定义 2.3 滥用网络层 2.4 网络层回应 第3章 传输层的攻击与防御 3.1 使用iptables记录传输层首部 3.2 传输层攻击的定义 3.3 滥用传输层 3.4 传输层回应 第4章 应用层的攻击与防御 4.1 使用iptables实现应用层字符串匹配 4.2 应用层攻击的定义 4.3 滥用应用层 4.4 加密和应用层编码 4.5 应用层回应 第5章 端口扫描攻击检测程序psad简介 第6章 psad运作：检测可疑流量 第7章 psad高级主题：从签名匹配到操作系统指纹识别 第8章 使用psad实现积极回应 第9章 转换Snort规则为iptables规则 第10章 部署fwsnort 第11章 psad与fwsnort结合 第12章 端口碰撞与单数据包授权 第13章 fwknop简介 第14章 可视化iptables日志 附录A 攻击伪造 附录B 一个完整的fwsnort脚本

<<Linux防火墙>>

章节摘录

第1章 iptablesE用简介 1.1 iptables iptables防火墙由Netfilter项目开发（<http://www.netfilter.org>），自2001年1 Linux 2.4内核发布以来，它就成为Linux的一部分了。

多年来，iptables发展成为一个功能强大的防火墙，它已具备通常只会在专有的商业防火墙中才能发现的大多数功能。

例如，iptables提供了全面的协议状态跟踪、数据包的应用层检查、速率限制和一个功能强大的机制以指定过滤策略。

所有主流的Linux发行版都包含了iptables，而且许多发行版在系统安装过程中就提示用户部署iptables策略。

Linux社区的一些人未弄清术语iptables和Netfilter之间的差别，从而产生某些混淆的概念。

由Linux提供的所有包过滤和包修改设施的官方项目名为Netfilter，但这个术语同时也指Linux内核中的一个框架，它可以用于在不同阶段将函数挂接（hook）进网络栈。

另一方面，iptables使用Netfilter框架旨在将对数据包执行操作（如过滤）的函数挂接进网络栈。

你可以认为Netfilter提供了一个框架，iptables在它之上建立了防火墙功能。

<<Linux防火墙>>

媒体关注与评论

我看过数百部安全技术方面的著作，但本书可谓出类拔萃，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！

——Richard Bejtlich，通用电气公司应急响应部主管，著名安全技术专家 强烈推荐！
内容极为实用，揭示了大量网络攻击检测与处理的技术内幕。

——John Vacca，著名安全技术专家，Firewalls：Jumpstart for Network and Systems Administrators

<<Linux防火墙>>

编辑推荐

《Linux防火墙》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。

<<Linux防火墙>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>