第一图书网, tushu007.com

<<Linux 服务器安全策略详解>>

图书基本信息

书名：<<Linux 服务器安全策略详解>>

13位ISBN编号：9787121086809

10位ISBN编号：7121086808

出版时间：2009-6

出版时间：电子工业出版社

作者：曹江华

页数：769

字数：1304000

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

前言

Linux系统属于开放源代码软件，由于Linux系统具有稳定、安全、网络负载力强、占用硬件资源少等技术特点，自问世以来得到了迅速推广和应用，并已发展为当今世界的主流操作系统之一。
目前对Linux感兴趣的用户主要集中在一些垂直行业当中。
在国外，企图提升利润率的有零售、家电行业，包括石油、动画设计等在内的计算密集型应用企业，还有想通过Linux的成本控制来提高企业竞争优势的一些电信、政府和医疗行业。
对于零售行业的POS终端和数据中心而言，Linux既可靠又便宜。
石油行业则通常利用上千个结点的Linux集群来承担石油勘探中的大量运算工作。
国内的企业应用同样也迅速普及。
由于电子政务的“崛起”，政府行业已占据了Linux市场的大量份额。
能源行业的Linux应用在国内市场份额上也名列前茅。
金融、电信等传统大行业应用Linux的趋势已然显露。
可以总结出Linux的擅长应用领域是：　1. 单一应用的基础服务器，如DNS和DHCP服务器、Web服务器、防火墙、文件和互联网代理服务器。
2. 界定清晰，与其他系统没有交叉的应用。
3. 高性能计算及计算密集型应用，如风险分析、数据分析、数据建模等。
4. 中小型数据库。
对于那些应用很单纯的企业，购买Linux软件的成本优势则十分明显。
与Windows系列相比，Linux令人欣慰的一点是其出色的安全性，可以降低管理成本。
这也是使很多公司转向Linux的一个非常重要的原因。
在Windows服务器上，补丁让人应接不暇，耗费大量时间和精力。
于是，人们选择了Linux。
尽管Linux也会受病毒和黑客的侵扰，但是Linux内核毕竟是由众多具有黑客背景的程序员逐步完善而来的，相对安全一些。
目前，关于Linux方面的书虽然较多，但大多数都是介绍如何安装，以及如何使用像KDE和GNOME这类图形界面的，对Linux作为服务器应用的介绍相对较少，Linux真正的优势和发展方向是作为服务器操作系统。
根据需要，Linux可安装成各种各样的服务器。
Linux是一个十分稳定的操作系统，目前用户已逾千万。
但是，Linux服务器是否安全，这对Linux的用户来说是十分关心的问题。
本书的目的，就是要说明Linux服务器通过加固配置后是安全的。
第2版说明　本书第1版在2007年7月出版后，得到广大读者的关注，同时也得到一些热心读者的宝贵意见和反馈。
所以在第2版中做了一些内容的添加和删除。
在第8章FTP服务器安全策略部分删除了现在Linux平台应用比较少的Wu-ftp和ProFTPD 两种服务器的内容。
从21章开始是第2版添加的主要内容，首先使用三章的篇幅详细论述了两大开源数据库MySQL和PostgreSQL安全策略。
然后以此介绍了Linux下新闻组服务器构建、网络钓鱼的防范、Linux无线网络构建及其安全策略、使用Linux安全审计以及使用Selinux保护Linux服务器的方法。
附录部分笔者介绍了Linux服务器应急响应的流程与步骤。
限于本书的篇幅已经比较多了，关于虚拟化、集群、Web 2.0 等内容本书没有介绍，对此感兴趣的读者可以查看笔者的《Red Hat Enterprise Linux 5.0服务器构建与故障排除》。
另外对于第1版的附录也做了较大的修改。
删除了Linux命令的介绍，这么做的原因是考虑到目前已经有专门介绍Linux命令的相关图书，于是这里笔者节省了宝贵的篇，对此感兴趣的读者可以查看笔者的《Linux系统最佳实践工具:命令行技术》

。

内容概要

“ Linux就是服务器，或者换句话说，是服务器成就了Linux。
”相信读者对于这样的判断肯定会有不同意见。
这里不是以偏概全，只为强调Linux与服务器与生俱来的天然联系。
实际上，对于Linux厂商而言，约90%以上的收入都来自服务器应用市场。
Linux主要用于架设网络服务器。
如今关于服务器和网站被黑客攻击的报告几乎每天都可以见到，而且随着网络应用的丰富多样，攻击的形式和方法也千变万化。
如何增强Linux服务器的安全性是Linux系统管理员最关心的问题之一。
　本书共28章和1个附录。
概括而言，实质是五部分内容：第一部分分级介绍对Linux服务器的攻击情况，以及Linux网络基础；第二部分是本书的核心，针对不同的Linux服务器分别介绍各自的安全策略；第三部分介绍Linux服务器的安全工具；第四部分是Linux下开源数据库安全以及Linux下新闻组服务器构建、网络钓鱼的防范、Linux无线网络构建及其安全策略、使用Linux安全审计以及使用SeLinux保护Linux服务器的方法；第五部分是1个附录，介绍Linux服务器应急响应流程与步骤。
　本书适合作为大专院校计算机专业师生的教材或教学参考书，也适合于Linux网络管理员和系统管理员，以及对安全方面感兴趣的读者。

书籍目录

第1章　Linux网络基础与Linux服务器的安全威胁　第2章　OpenSSL与Linux网络安全第3章　PAM与Open LDAP第4章　Linux网络服务和Xinetd第5章　DNS服务器的安全策略第6章　Wed服务器的安全策略第7章　电子邮件服务器的安全策略第8章　FTP服务器的安全策略第9章　Samda服务器的安全策略第10章　NFS服务器的安全策略第11章　DHCP服务器的安全策略第12章　Squid服务器的安全策略第13章　SSH服务器的安全策略第14章　Linux防火墙　第15章　Linux网络环境下的VPN构建　第16章　使用IDS保护Linux服务器第17章　Linux网络监控策略第18章　Linux常用安全工具第19章　防范嗅探器攻击和Linux病毒　第20章　Linux数据备份恢复技术第21章　数据库简介Linux开源数据库安全现状第22章　MySQL数据服务器安全第23章　PostgreSQL数据库服务器安全第24章　搭建Linux新闻组服务器第25章　在Linux网络环境下防范网络钓鱼第26章　Linux无线网络构建及其安全策略第27章　Linux安全审计系统　第28章　使用Linux系统附录A　Linux服务器应急响应流程与步骤

章节摘录

第1章 Linux网络基础与Linux服务器的安全威胁 1.1 Linux网络基础 1.1.1 Linux网络结构的特点 Linux在服务器领域已经非常成熟，其影响力日趋增大。
Linux的网络服务功能非常强大，但是由于Linux的桌面应用和Windows相比还有一定差距，除了一些Linux专门实验室之外，大多数企业在应用Linux系统时，往往是Linux和Windows（或UNIx）等操作系统共存形成的异构网络。
在一个网络系统中，操作系统的地位是非常重要的。
Linux网络操作系统以高效性和灵活性而著称。
它能够在PC上实现全部的UNIX特性，具有多任务、多用户的特点。
Linux的组网能力非常强大，它的TCP／IP代码是最高级的。
Linux不仅提供了对当前的TCP／IP协议的完全支持，也包括了对下一代Intemet协议IPv6的支持。
Linux内核还包括了IP防火墙代码、IP防伪、IP服务质量控制及许多安全特性。
Linux的网络实现是模仿FreeBSD的，它支持FreeBSD的带有扩展的Sockets（套接字）和TCP／IP协议。
它支持两个主机间的网络连接和Sockets通信模型，实现了两种类型的Sockets-BSDSockets和INET Sockets。
它为不同的通信模型提供了两种传输协议，即不可靠的、基于消息的UDP传输协议和可靠的、基于流的TCP传输协议，并且都是在IP网际协议上实现的。

编辑推荐

详细介绍了Linux下最主要服务器的安全策略，几乎涉及所有主流Linux擅长的领域，弥补了国内图书在Linux安全领域的空白。
针对服务器领域使用最为广泛的红帽企业版，同时兼顾一些Linux发行版。

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