安全可以复制——向世界500强企业学习Linux安全管理与运维之道

51CTO真心推荐：献给工作在企业信息安全和Linux安全运维领域工作者的实用宝典。

李洋 编著

防线

企业Linux安全运维理念和实战

“一本真正适合中国企业的Linux安全管理与运维书籍”

“站在巨人肩膀上学习企业信息安全建设和Linux安全运维”

- 企业安全架构设计和原则
- 企业安全技术实战演练
- 企业安全标准和审计指导
- Linux安全管理和运维实现
- Linux开源安全运维工具和应用

清华大学出版社


防线
企业Linux安全运维理念和实战
李 洋 编著
清华大学出版社

内 容 简 介

本书作者有多年的世界500强企业的信息安全管理工作经验，深谙500强企业信息安全建设、规划、实施和管理的细节、难点和重点问题。世界500强企业对于信息安全工作的重视程度，对于信息安全在建设、规划、实施和管理等方面都有其独到之处，可以为其他中小型和大型企业所借鉴和参照。基于这个目的，本书以笔者在500强企业中使用企业级开源操作系统Linux在信息安全中的部署和使用方法为切入点，来介绍如何做好信息安全工作。

本书共分为5篇，包含19章和两个附录。面向企业实际需求，对如何使用企业开源Linux操作系统来进行信息安全建设进行了全面、深入和系统的分析，并通过大量的威胁分析、解决思路、解决技术及实现实例来进行介绍。

本书覆盖知识面广，立意较高，几乎覆盖了企业应用开源Linux系统进行信息安全建设的方方面面。

本书适用于信息安全从业人员、众多Linux爱好者、IT培训人员及IT从业者、企业高级管理人员(CIO、CEO、CSO等)，并可作为高等院校计算机和信息安全专业学生的教学参考用书。

图书在版编目(CIP)数据

防线：企业Linux安全运维理念和实战 / 李洋编著. .—北京：清华大学出版社，2013

ISBN 978-7-302-31807-1

Ⅰ.①防… Ⅱ. ①李… Ⅲ. ①Linux操作系统—安全技术 Ⅳ. ①TP316.89

中国版本图书馆CIP数据核字（2013）第062997号

责任编辑：栾大成
封面设计：杨玉芳
责任校对：徐俊伟
责任印制：沈　露

出版发行：清华大学出版社
　　网　　址：http://www.tup.com.cn，http://www.wqbook.com
　　地　　址：北京清华大学学研大厦A座　　**邮　　编**：100084
　　社 总 机：010-62770175　　**邮　　购**：010-62786544
　　投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
　　质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：北京世知印务有限公司
装 订 者：三河市溧源装订厂
经　　销：全国新华书店
开　　本：188mm×260mm　**印　张**：39　**插　页**：1　**字　数**：1081千字
版　　次：2013年8月第1版　　**印　次**：2013年8月第1次印刷
印　　数：1～3000
定　　价：79.00元

产品编号：043915-01

前 言

本书的写作思路

人的正确思想是从哪里来的？——什么是安全（What）

“人的正确思想是从哪里来的？是从天上掉下来的吗？不是。是自己头脑里固有的吗？不是。人的正确思想，只能从社会实践中来，只能从生产斗争、阶级斗争和科学实验这三项实践中来。”毛泽东同志早在1963年5月就英明地作出过上述论断。

在写这本书之前，我就一直在思考这个问题，什么是安全？安全如何定义？安全的定义来自于哪里？……种种疑问，一直陪伴着我。进入信息安全行业已经10多个年头了，从技术研发，学术研究到目前的企业信息安全规划、管理、决策，大大小小的项目，层出不穷的安全威胁，琳琅满目的安全产品，日新月异的安全市场，如雨后春笋般出现的安全新名词，都使我更加坚定地意识到，在这本书里，必须把安全这个问题讲透彻，讲明白。在市面上很多书籍里面，包括操作系统安全、安全原理方面的书籍，以及我以前的几部著作中，都忽略了这个问题，这个问题没有阐述和介绍清楚，会直接影响到企业的信息安全工作的定位、实施和成效。

因此，在这本书的前面章节中，笔者结合目前业界最新的研究成果和自己10余年的信息安全从业经验，并根据著名信息安全领域专家方滨兴院士科学、系统定义的信息安全概念，作了有针对性地扩展和延伸，给出了信息安全定义、企业信息安全框架以及企业信息安全实施和建设的主要工作思路。有了这个前提，在后面章节的介绍中就有了一个科学的基调和前提，也便于向读者介绍500强企业使用开源Linux系统建设信息安全的思路和具体方法。

打破砂锅问到底——500强企业为什么要关注安全（Why）

本书的笔者有多年的世界500强企业的信息安全管理工作经验，深谙500强企业信息安全建设、规划、实施和管理的细节、难点和重点问题。并且，笔者认为，世界500强企业对于信息安全工作的重视程度，以及信息安全在建设、规划、实施和管理等方面都有其所长，可以为其他中小型和大型企业所借鉴和参照。基于这个目的，本书以笔者在500强企业中使用企业级开源操作系统Linux在信息安全中的部署和使用方法为切入点，来介绍如何做好信息安全工作。

言归正传，500强企业为什么要关注安全呢？原因是多方面的。首先，500强企业有自己的服务器、操作系统，也有自己的系统，这些系统无论是为内部员工服务的（比如OA系统、电子邮件系统等），还是为外部客户服务的（比如Web发布系统、线上业务系统等），都会面临多方面的安全威胁，包括内部员工的恶意破坏、数据泄露、误操作等，以及外部不法用户的非授权访问、拒绝服务攻击、垃圾邮件、SQL注入等，这些都需要进行安全方面的全面分析、研究、部署等．才能

将这些威胁对于企业的危害降到最低；其次，作为大型企业来说，需要从体制上来健全信息安全工作，包括规划、实施、流程制定、人员培训等，所以要特别关注信息安全。实践证明，越是规模大的企业，越容易出现安全问题，如果不居安思危，早作准备，就很难在现代企业中立于不败之地，也很难幸免于我们最近经常听到的密码泄露事件、客户资料泄密事件等。一旦遇到这些问题，企业的形象将会不保，企业的品牌和对于用户建立的信任也会受到很大影响；最后，国家、政府和行业也对不同的企业提出了很多信息安全方面的管制要求，主要是满足合规、生产安全等方面的要求，比如著名的国家等保、证监会/银监会的要求、支付行业的 PCI/DSS、美国的 SOX 法案等，都对企业尤其是大型企业提出了非常好的安全要求。

实践出真知——500 强企业如何做好信息安全建设（How）

明白了什么是安全，为什么要关注安全，那么最重要的一步就是如何来做安全了，也就是如何通过技术和管理手段来保证企业的安全，防止安全事件或者事故的发生，树立企业形象，保证企业正常运行。

根据笔者在 500 强企业的多年信息安全工作经验，在本书中，将使用企业级 Linux 进行信息安全建设工作的具体实施方法分为以下 5 个阶段：

1. 认知阶段；
2. 梳理阶段；
3. 实施阶段；
4. 运维阶段；
5. 工具应用阶段。

这 5 个阶段直接对应到本书的 5 个技术部分。会系统、全面地向读者介绍 500 强企业作好信息安全工作的方方面面。

读者群

本书是一本面向企业的基于操作系统平台进行信息安全建设的实践书籍，是围绕着什么是、为什么和怎么样构建信息安全来进行介绍的。因此，这本书并不需要读者具有高深的计算机科学与技术或者信息安全的基础理论知识，这本书的主要读者是怀有一定的工作目标并对信息安全有一定兴趣的工程师或者信息安全从业人员。

笔者也非常希望企业的 CIO、CEO 和 CSO 都能够从本书中获得他们需要的一些宝贵理念和实践指引。本书中的一些理念、方法和实践指南，笔者都在企业信息安全建设中与一些 CIO、CEO 经过讨论并达成共识。

刚走出校门的大学生、研究生，以及正在通过各种渠道（包括培训、实习等）来试图进入信息安全领域的学子或者工作者，相信可以从本书中获得系统的知识和工作的指南。本书中所阐述的知识、操作所用的案例都是在实际工作中精挑细选的，相信读者可以从中提前感受和体会到作为一名信息安全从业人员所需要具备的基本知识结构以及实际的技能。

作者简介

本书的笔者有多年500强企业从事信息安全技术研发和管理的实践经验，擅长于Linux安全的管理和研发，具有深厚的Linux安全基础理论知识和丰富的项目经验。本书由李洋主持编写，参与编写的作者还有柴泽楠、靳文佳、张晓明、江扬旺、康宇、宋继阳、吴廷勇、张恒、孙定隆、陈义勇、石依山、姚笃君、李刚、王博、李淞洋、吕远、孙悦、张雷、史思冰、田源、关威等。

由于作者水平有限，书中难免存在疏漏与不当之处，敬请专家和广大读者给予批评指正。欢迎大家通过我的51CTO官方blog（http://patterson.blog.51cto.com/）以及新浪微博（http://weibo.com/u/2358007797）与我互动交流。

内容编排

在内容的编排上，本书精挑细选，摒弃了企业应用小众化的FTP、Samba、NFS等，浓墨重彩在500强企业关注的信息安全框架、数据安全、通信安全、移动办公安全等专题上面。本书各章的内容安排如下。

第1篇（安全运维理论及背景准备）——“知己知彼，百战不殆”

第1章是本书的入门知识。对于一个500强企业的信息安全管理者来说，必须要对国际、国内的信息安全现状，尤其是企业信息安全面临的威胁，以及所面对的对手——黑客，都要有一个非常清醒的认识，本章即对这些内容进行入门性的介绍。

第2章分门别类地详细介绍如何在各个层次来使用信息安全的相关技术来应对安全威胁。

第2篇（企业Linux安全运维规划及选型）——“凡事预则立，不预则废”

第3章介绍企业的信息安全工作的思路，以及具体的Linux安全的实施内容。

第4章介绍企业在选择时要考虑到其发行套件、内核版本以及服务器选型等诸多问题。并且介绍如何解决为了节省人力、物力，而大规模地高效部署Linux的问题。

第3篇（企业Linux安全运维实战）——“战略上藐视敌人，战术上重视敌人”

第5章从文件系统、进程、用户管理、日志安全四个方面出发，介绍企业对于这四个方面的安全防护技术、工具和策略。

第6章针对目录/文件的访问控制方式，介绍更为灵活的通过访问控制列表（ACL）以及SELinux的企业Linux安全加固机制。

第7章详细介绍企业如何通过紧密布控，全面地保证开源企业Web服务器运维安全。

第8章从分析基础网络服务面临的安全风险出发，给出如何对这些服务进行安全防护的方法和技术。

第9章介绍如何使用数据防泄露、加密技术和工具保障企业数据安全。

第10章介绍VPN技术的基本原理和分类，并深入分析和探讨如何使用开源的VPN技术来保障企业的移动数据通信安全。

第11章详细介绍企业如何应用相关的工具来进行企业Linux服务器远程安全管理。

第12章针对Linux网络，介绍企业网络流量管理的主要技术、理念和工具。

第 13 章详细介绍企业级防火墙的部署及应用。

第 14 章详细介绍企业立体式入侵检测及防御体系、技术及工具的应用。

第 4 篇（企业 Linux 安全监控）——“师夷长技以制夷”

第 15 章介绍企业 Linux 系统及性能监控的常用工具和方法，并通过大量的实例来揭示企业是如何进行此项安全运维工作的。

第 16 章介绍如何使用优秀的开源网络监控工具辅助网络管理人员和信息安全工作人员进行网络监控和管理。

第 17 章介绍如何在 Linux 系统下通过端口和漏洞扫描来发现企业网络漏洞，从而为安全工作者提供相应的素材，以针对具体信息采取相应的措施来对该漏洞进行修补等。

第 5 篇（企业 Linux 安全运维命令、工具）——“工欲善其事，必先利其器”

第 18 章对企业级 Linux 内核配置、编译、安装、系统恢复等细节性的问题进行详细介绍。

第 19 章对一些比较常用的优秀开源工具进行介绍。

附录 A 挑选了百余种 Linux 中最为常见和重要的命令，给出的这些命令的功能说明和参数，以及语法使用都是严格地根据 Linux 中的 man 手册参考得来的，希望为用户提供日常使用和学习的参考之用。

附录 B 为读者提供了一些在企业信息安全管理中可能用到的非常有用处的网络工具。

致谢

作者首先由衷地感谢清华大学出版社的资深编辑栾大成为本书出版所作的大量耐心、细致的工作，他对本书的系统性、严谨性和科学性方面提了大量宝贵的意见；还要感谢父母和妻儿对我的支持，尤其是我可爱的女儿，他们给我的生活带来了太多的快乐和色彩，没有他们，这本书也不可能成功问世。

回复信息安全爱好者的一封信

来信

李博士您好，期望百忙之中能浪费您一些时间，关于追求技术的矛盾：

很早就关注了您的 blog，您发表的很多文章都值得借鉴，令我钦佩。正在研读您的《网络协议本质论》，巩固知识体系！开门见山，首先介绍下我自己，我是一个执着于追求技术的人，两年前，因为信息安全专业而去了一所大专院校学习。现在，两年过去了，也学到了一些基础知识，不过还没形成体系，而且偏向网络这一块，下面把这两年我所自学的东西列出来：

1．网络方向：网络基础、TCP/IP（仅原理，代码实现未研究），思科的 CCNA、部分 NP+模拟器实践，考取了软考的网络工程师中级职称证书，考这个证书的主要目的是为了把网络的整个知识体系打下一个框架性的认识，力争融会贯通。

2．操作系统方向：熟悉 Linux、RHCE、各类服务搭建、Linux 下 ShellScript 的编写（服务器运维）、操作系统原理、Server 2003、数据库等。

3．Web 安全方向：ASP/PHP/JSP 及一些脚本编写、网站攻防、渗透测试等（这一块还没开始）。

4．编程方向：C/C++/汇编等（停留在皮毛阶段，主要精力花在了网络技术和服务器（Linux）应用技术这一块）。

学习定位：

1．主攻 Linux，掌握常用命令的用法，熟悉 Shell 脚本的编写，能高效搭建各种常用服务及安全。（60%精力）

2．掌握汇编语言/C/C++的基础，有时间+数据结构。（20%精力，上半年）

3． 完成任务 2 后开始学习 Web 安全、渗透等攻防技术，部分可归纳在 Linux 学习范围内。（30%精力、下半年）

4．熟悉网络设备的配置及技术原理，至少有个感性的认识，如多区域 OSPF、VPN、MPLS 和防火墙。（10%精力）

大概就是这些，路几乎都是自己摸索出来的，与任晓辉的那张黑客分类进阶图的网络攻防方向差不多，这条路似乎有些偏离安全技术的核心方向，如逆向、反汇编调试、脱克、破解、外挂、反病毒、木马、内核编写等底层的东西，但真正要把这些东西学通，又需要相当长的时间去掌握，而我要面对现实问题，半年后差不多就要去相关的工作岗位应聘，做一些偏向网络应用方面的技术，必须先站稳脚跟，找到谋生的手段，出校门后会先做一些 Linux 服务器的运维相关工作来作为过渡职位，可能偏向网站安全，先以 Linux 为主攻方向，然后利用空闲时间学习安全技术，包括 Linux 内核，并把安全这个知识面打好，比如学习 CISP 的课程体系，虽然广而不精，重理论、概念性知识，缺少实践，但我觉得形成一个比较广的安全知识体系并深入研究技术会更好些，然后转而做一些信息安全的相关工作（应该是涉及面比较广的，而不是纯做某一项技术的大牛，比

如内核、逆向、软件安全、反病毒软件编写等），也许技术涉及的不深，但这样的方向也是出于我自身的各种因素及发展而理性判断而决定的，黑客这些核心技术，我想作为一种业余爱好去研究（也许能在工作中作为辅助甚至转为优势）。事实如此，不过心有不甘，我也想做到技术的巅峰，以致经常产生矛盾心理，不知道前辈是如何衡量这些现实因素的？

我渴望黑客、安全技术的最高境界，只因起步较晚，能力有限，马上要面临现实生存问题，所以必须想个办法，两年来，我主要精力花在网络这一块（虽然本质上都是相通的，但也需有所侧重嘛），所以我的方向是先以网络安全为主，具体点，应该是 Linux 系统管理员，一个服务器架设与确保服务安全的管理员，然后倾向 Web 安全，以这个作为成为“大牛”的一个跳板，一个暂时的安身之地，算一个比较折中的方向吧，我觉得做这一块，既要懂操作系统、网络、数据库、C、汇编，还要懂计算机组成原理、脚本语言、算法、逻辑思维等，才能把 Linux 学得比较好，我想，花几年时间，等 Linux 做到一定程度，编程基础也相应上来了，那么就可以深入它的内核，读它的内核源代码，深入底层的学习，不代表未来就不往黑客的核心技术发展，包括软件安全，但我必须先花几年时间把“网络安全”这一块做好，做得比较“精通”（业余时间学软件安全技术）。

我就把应用性技术比作“外功”，而把底层技术，比如汇编，比作“内功”，只剩半年多时间，我需要先把“外功”练好，毕业后找个容身之地，然后利用运维工作较多的空闲时间，去修炼“内功”。

近期目标：力争做一个优秀的 Linux 系统管理员，服务器安全、架设这一块，先以 Web 安全为主。

但我会先花时间掌握编写高效的运维脚本能力，即 Linux 下的 ShellScripts，进一步了解 Linux 的工作原理，以致节省工作时间，然后利用这些空闲时间去学习黑客所需要的技术知识，比如 C、汇编、数据结构与算法等重要的基础知识，Web 安全要做好，又要懂数据库，比如 Oracle。

具体岗位：比如维护百度、淘宝等门户网站的安全。

期望李前辈能在百忙之中花一些时间来帮我理清下思路与矛盾，从内心感激您，谢谢！

一名追求提高技术实力而获得成就感和满足、不断奋斗中的所谓的“信息安全学子”的来信。

我的回复

这位朋友，你好！

看了你的信，我非常高兴，你能够在信息安全的这条道路上默默探索，慢慢前进，非常不容易，值得肯定！

下面我帮你理清一下思路。其实你的情况非常典型，很多号称在信息安全领域搞了多年的人，也没你想的这么多，这么透彻，我非常高兴，中国的信息安全人才还是不缺乏的。建议你从如下几个方面着手学习和发展。

（1）打牢基础，注重积累

信息安全方面涉及的领域非常广，本质上是一个交叉性学科，涵盖的内容包括操作系统、计算机网络、数据通信、数据库、密码学、程序语言与设计、编译原理、计算机体系结构等，而且对每一门的要求都不低，至少要理解原理，并能够举一反三。所谓安全，主要的就是敏锐的洞察力和判断力，使用这些基础知识去对系统、软件、网络、应用等进行安全与否的判断以及提出解决办法，是一个非常综合性的工作。因此，基础打得牢不牢，知识面广不广，直接决定了你以后的发展。可以多买一些基础性的结合应用的书籍来看，这样既不会枯燥乏味，也能迅速提高自己，我写的一些书籍大多都是两者结合，你可以参考使用。

（2）勤于实践，多多动手

信息安全同时又是一门实践性和操作性非常强的学科，从你所用的一些工具软件、反汇编技术等，都需要实践。当然，这个实践不能盲目地从网上下载一些工具，拿来就用。需要理解其原理、特性和用途，才能有的放矢，也能迅速提高。这就需要以自己牢固的基础知识为后盾，切忌盲目、好高骛远，一心只想使用工具，而忽略了自己在各方面的沉淀和积累。现在的工具非常多，但是切忌不要进行恶意的攻击行为，可以采用虚拟机等在虚拟的环境中进行，这是一个前提，也是一个信息安全工作人员的职业操守。

（3）善于总结，醍醐灌顶

工作这么多年，从数十个国家几千万项目的信息安全研发工作到近年来大型企业的信息安全管理工作，我最大的收获就是要善于总结，阶段性地总结。各类应用不断出现，其漏洞和风险越来越多，所暴露的安全问题也越来越多，是“头痛医头，脚痛医脚”，还是总结得出一些好的方法，对一类问题的解决办法或者解决方案效率高呢？显然是后者。但是做起来不是那么容易的，需要有前面基础学习和实践经验甚至教训的总结。现在中国信息安全的格局比较混乱，很多所谓的信息安全工作人员只注重一朝一夕的工具的使用、一次两次的所谓“攻击实战”，却不注重方法，不注重总结，这是非常低效的。可以看到，国外的信息安全从业人员，都有非常深厚的基础功底和实践经验，这值得我们好好借鉴。这样，经过一段时间，你就会有醍醐灌顶、豁然开朗的感觉，你就慢慢进步了，慢慢地朝着正规的、良性的方向发展。

因此，根据上面几个原则，相信不难规划你的信息安全之路，祝你学业有成！

李 洋

推 荐 序 一

“结识李先生已经 6 年有余了。从一名技术媒体人的角度来看，本书既不是空洞的纸上谈兵，也不是无来由的蠢蠢冒进，而是李先生在多年的工作和研究中所积累的理论和经验。

开源是所有的 IT 爱好者所热衷的话题，但是如何将开源合理、安全地利用到企业信息化建设，如何高质量地针对开源进行维护，如何利用开源有效地抵御和防范日渐增强的企业信息化威胁，诸如此类的问题是企业级信息化管理者需要不断攻克的一个课题。而本书正是为这些企业级信息化管理者带来了一套切实可行的方式方法。在此向各位读者朋友推荐这本书籍，也祝愿李先生的作品能够让更多的读者从中得到收获。

——51CTO 网站副总编赵磊先生

推 荐 序 二

安全问题，是这两年不断引爆人们神经的话题，从 QQ 诈骗，到某网站礼品卡被盗用，再到国内知名 IT 论坛用户名密码泄露，人们的信息安全和财产安全面临着一次又一次的危机，而发生这些事情后，我们第一个反应到的词是什么？是安全！

当我打开这本书的时候，看到的不是“一雨池塘水面平，淡磨明镜照檐楹”，而是“醉卧沙场君莫笑，古来征战几十还”，在系统一次次被攻陷，多少人陷入“但使龙城飞将在，不教胡马度阴山”的场景。没有刀光剑影的江湖，就不叫江湖。同样没有你攻我防的网络，也不是网络。网络的本意就是将大家的信息孤岛互相联系起来，融入一网，而称为互联网。而在这个圈子里面，总有人不甘寂寞，喜欢窥探其他人的“岛屿”。于是大家自愿自发地组建了生态圈自卫队，而这本书，我认为是自卫队的必读教材。

现在多数的书籍要么把重点都放在了概念阐述或者是学术理论上，忽略了实际操作的疑惑和应用难题的解决；要么将运维说得概念大到天，忽略了运维的真正意义。而该书打破了这种常规思路，给读者耳目一新的感觉。这本书是一本着眼于现在企业安全管理难题的实用型工具书。其理念对于企业 IT 管理人员具有指导意义，在使用任何工具前，翻阅一下这本书，它会告诉你在新系统上线前，可能会遇到哪些问题；也会告诉你在上线后，可能会受到哪些攻击。这本书以 Linux 为平台，详细讲述了安全运维理念中最为核心的方法。应用普及到安全边界、身份安全与访问管理、数据保密以及安全监控和管理等，几乎无所不容。

李洋已经在安全领域从事 10 余年，一直致力于计算机网络信息安全的研发工作，现任一家国际知名投资银行的资深信息安全顾问和架构师，同时担任 ICC、IEEE Communications Letters、Globecom、Elsevier Computer Communications、Elsevier Computers Security 等多种 SCI 检索期刊和国际著名会议的审稿人和 TPC，并在国家 863、国家自然科学基金、国家 242 信息安全计划项目等项目中作为主要成员，为项目组做出了显著贡献。他对于计算机安全技术和解决方案有着高度的热情和执着，这种热情和执着作为他生命中的特质伴随其职业生涯。也正是这种特质，使他

获得了大量的学术认可和项目成果，他在安全领域的大量著作就是他这种特质的一个缩写。李洋在网络安全领域拥有丰富的阅历，在写作方面也有着出众的引导读者的能力，经过他性格特质的加工，使得该书必然是一部海纳百川的书。如果您正在为公司的安全问题担忧，不妨考虑一下这本书，该书给读者带来的将不只是知识的累计和经验的提升，还希望读者在遇到问题的时候，通过这本书可以“众里寻他千百度，蓦然回首，答案只在桌上手边处”。

——汇美国际下属科技公司 CTO 战剑新先生

推 荐 序 三

Network security has been becoming the cornerstone of modern information system. With the widespread deployment of Cloud technology facilities and the extensive application of electronic settlement and payment in the field of finance service, this trend is accelerating, thus from this aspect, security has been at the heart of corporate information system.

Doctor Yang Li has been a senior expert with extensive experience in network security. This book is his another masterpiece in security field which is almost rated as the perfect combination of security theory and practice, to some extent, it is a bible book of security.

WORTHWHILE READING!!!

——Andrew Liu, the CTO of Mobile Payment Inc. @Silicon Valley

目 录

第一篇 安全运维理论及背景准备

第二篇 企业 Linux 安全运维规划及选型

第三篇 企业 Linux 安全运维实战