Broadview
www.broadview.com.cn

从菜鸟到Linux安全专家

◎ 李洋 编著

電子工業出版社
http://www.phei.com.cn

蜕变：
从菜鸟到Linux安全专家

◎李洋 编著

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内容简介

本书通过实际故事场景对Linux安全技术和应用方法进行了全面、深入和系统的分析。分别从黑客攻击的基本技术、Linux面临的安全威胁、Linux系统安全管理、Linux网络服务安全管理、Linux核心安全技术等多个层面，向读者系统、全面、科学地讲述了与Linux相关的原理、技术和机制等安全方法。

本书覆盖的知识面广，基本覆盖了Linux安全的方方面面。本书适用于广大读者群，包括众多Linux安全爱好者、中高级Linux用户、IT培训人员及IT从业者，同时也兼顾网络管理员。本书也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

蜕变：从菜鸟到Linux安全专家 / 李洋编著. —北京：电子工业出版社，2011.9
ISBN 978-7-121-14434-9

Ⅰ. ①蜕… Ⅱ. ①李… Ⅲ. ①Linux操作系统—安全技术 Ⅳ. ①TP316.81

中国版本图书馆CIP数据核字（2011）第172688号

策划编辑：张春雨
责任编辑：李云静
特约编辑：孙佳志
印　　刷：北京天宇星印刷厂
装　　订：三河市皇庄路通装订厂
出版发行：电子工业出版社
　　北京市海淀区万寿路173信箱　　邮编：100036
开　　本：787×1092　1/16　　印张：30.75　　字数：787.2千字
印　　次：2011年9月第1次印刷
印　　数：4000册　　定价：75.00元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至zlts@phei.com.cn，盗版侵权举报请发邮件至dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

写作目的

“我是一名刚毕业的大学生，想从事Linux安全管理工作，不知道要学些什么？”

“很多企业目前都使用Linux，那么Linux安全怎么管理，要用到哪些技术？”

“我没有很好的学历，学习Linux安全合适吗？能成为合格的Linux安全专家吗？”

……

很多读者通过Blog、邮件、IM等方式与我沟通，问得最多的就是Linux安全方面的问题。学什么，如何学，如何快速地学，如何学以致用，这些都是他们所关心的问题。并且，Linux系统的门槛确实很高，不像Windows那么容易上手和掌握。由于当前社会、企业以及院校对信息安全的关注度都很高，对Linux安全管理员、安全专家的就业需求也很旺盛，因此，有很多不大了解操作系统原理，没怎么接触过Linux的所谓“菜鸟”同志们也加入到学习的队伍中来。

笔者在信息安全、Linux安全管理领域已经摸爬滚打了十几个年头了，感觉非常有必要写这么一本书来奉献给初涉Linux安全领域的读者们，不但教会他们要用什么技术，而且通过一些小故事来教会他们如何应用这些技术，也就是所谓的安全理念。

总而言之，本书的写作目的是要说明以下几点。

（1）没有学历，也可以成为Linux安全专家。

（2）从菜鸟到Linux安全专家，没有不可逾越的鸿沟。

（3）学习Linux安全，学以致用是重点。

本书写作特色

随着黑客攻击问题的不断加剧，木马、病毒、网络钓鱼、分布式拒绝服务攻击、僵尸网络等网络威胁的不断涌现，信息安全问题已经成为国家、社会和企业关注的焦点问题。信息安全问题的范围已经扩展到计算机领域和通信领域的方方面面，其中作为基础软件的操作系统也不例外。Linux作为一种优秀的开源网络操作系统，在网络技术日益发展的今天，凭借其在安全性、稳定性等方面的巨大优势，正受到越来越多用户的青睐，一些大型的网络及网站服务器都建立在Linux平台之上。然而，其在系统管理、网络服务管理等方面的安全问题仍然不可小视。针对该系统的安全问题的分析和相应的安全技术保障，已成为

广大网络和系统管理员及众多操作系统用户的迫切需求。

放眼目前Linux安全技术书籍市场，不难发现，以特定版本Linux为主线进行讲述的书籍比较多，而且比较着重于技术本身。近一年多来，我一直跟电子工业出版社的多位编辑以及广泛的读者进行过很多次交流，一致认为，Linux安全在强调技术的同时，更加强调其应用场景和理念，即不但要解决能用什么技术，更要解决如何用和怎么用的问题，即不但要“授之以鱼”，更要“授之以渔”。原因很简单，在这个知识“爆炸”和Linux操作系统升级版本更新频繁的时代，相对于以前以技术和操作步骤为主流的灌输式论述方法来说，如何掌握知识的本质和有效应用才是当前读者关注的重点。

基于上述考虑，本书独树一帜，以一个刚从学校毕业，走向社会就业的大学生从底层管理员成为公司Linux安全专家成长历程的形式，运用幽默、风趣的故事表现手法，从Linux系统安全和Linux网络安全两个层面系统、全面地向读者介绍作为Linux安全管理员所应具备的方方面面的安全知识、安全原理和安全技能，主要包括Linux文件系统安全、进程安全、Web服务安全、FTP服务安全、防火墙、入侵检测系统等。同时，在故事中也穿插和渗透了关于这些Linux安全技术的应用场景、方法和原则，使读者在故事中全面、系统地掌握Linux安全的技术知识、应用方法和安全理念等。更重要的是，读者还能从故事主人公的职场成长历程中看到和学到Linux安全管理员、Linux安全专家的职业前景和发展轨迹。

本书面向众多的操作系统技术、网络技术工作者，包括系统管理员、网络工程师、网络管理员、网络安全工作者。本书亦可作为高等院校信息安全和操作系统方向的参考教材。

本书的作者有多年从事信息安全、Linux系统研究及开发的工作经验，在精心编写本书的同时还十分考究内容的编排、章节的组织以及讲解的方式，是作者多年理论研究和实践工作经验的结晶。本书由李洋主持编写，其他参与编写的作者还包括王俊丽、谷云、郭瑞、朱振华、魏铮、赵丹、朱耀、卢业伟、丁凡、叶靖、杨文勇、黄江洪、陈亮等，全书由李洋统一组稿和审校。当然，由于作者水平和时间有限，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。非常欢迎读者访问我的专家博客：http://patterson.blog.51cto.com/，与我进行交流互动。

本书内容

本书包括12章，并外加引子和1个附录。

引子：以故事为引子，介绍本书的开始情节和背景。

第1章：详细介绍Linux安全的基本理论和背景知识。

第2章：介绍企业级漏洞检测及防范的技术和工具。

第3章：整体、系统地介绍Linux系统防护中进程、文件、用户管理、日志管理的技术

和方法。

第4章：介绍构建安全DNS基础设施的相关技术和方法。

第5章：系统介绍安全构建Web服务器的方方面面。

第6章：详细介绍安全构建FTP服务器的技术和方法。

第7章：介绍安全构建邮件服务的技术和方法，包括垃圾邮件过滤和服务器安全配置等。

第8章：详细介绍代理服务的安全构建方法。

第9章：详细介绍远程监控和管理的技术和方法，包括SSH、VNC、VPN构建等。

第10章：介绍Linux系统下共享资源安全管理的方法，包括Samba、NFS等。

第11章：详细介绍Linux系统下使用IPtables开源防火墙构建网络安全的技术、理念和方法。

第12章：详细介绍Linux系统下使用Snort进行入侵检测的技术和方法。

附录A：推荐和介绍Linux系统下百余个常见的命令，供读者在实际工作中参考。

致谢

作者首先由衷地感谢电子工业出版社的编辑张春雨和符隆美，他们在我写书的过程中给了我无私的帮助。为了使本书能尽快与读者见面，他们花费了大量的心血和精力，并对本书质量和体系的把握起到了重要作用。除此之外，还感谢51CTO网站以及该网站安全频道资深编辑王文文为本书作出的贡献。

李洋

2011年8月于北京

目　录

菜鸟前传

小王是一个来自于南方的本科毕业生，年方23，计算机系毕业。怀揣着对首都北京的向往之情，他只身一人来到北京找工作。

先介绍一下小王的背景。小王在上学期间比较清闲，于是就自己攒了一台电脑，上上网，聊聊天，编编程，几年下来，虽然文化课成绩不怎么样，但是编程和网络技能长进不小。他很喜欢钻研黑客技术，比如病毒、木马、网络钓鱼等，并且还喜欢上一些网站与BBS，经常在那里学习和讨论。他尤其喜欢研究开源系统下的黑客以及安全技术，为什么呢？因为可以看到源代码。无论是Linux操作系统还是一些开源的黑客工具，他都能修改、使用，这也满足了小王的好奇心。因此，几年下来，小王也算是学校小有名气的“黑客”了。当然，小王并没有搞过什么破坏，据说在上大三的时候，小王发现一家私有企业网站有SQL注入攻击的风险，该企业网站为了奖励他，还给了他500元的奖金。

有了这些基础，小王想找一份能够发挥他专长的工作，这样一来可以提高自己的“黑客”技能，二来可以在开源系统下做一些安全方面的工作。所谓攻防，就是一场永不停止的博弈，小王想从攻与防中不断提升自己。

来到北京后，由于小王毕业的本科院校不是非常著名，因此很多著名的互联网企业都没有挑中他。其实小王的动手能力很强，但是由于上学时没有太注重基础知识的学习，因此一到面试和笔试环节，小王就被刷下来了，他为此感到很烦恼。

功夫不负有心人，经过2个多月的折腾，小王参加了大大小小40多场的招聘会，经过了几十场的面试，他终于被一家小型的网络公司录用为Linux安全运维工程师。

小王就这样开始了他的职业生涯……

第1章 上司训话：

网络安全态势分析

小王通过重重面试和考核，终于进入了这家网络公司。进公司的第一件事情就是向部门经理报到。部门经理是一个40岁左右的海归，对技术要求比较高，对公司安全管理的要求也很高。这不刚报到完并把手续办好，经理还没跟小王寒暄几句，就交给小王一项艰巨的任务——对网络安全态势作一个分析，小王只有硬着头皮上了，熬了整整3个通宵，终于拿出了一份比较完整的网络安全态势分析报告。