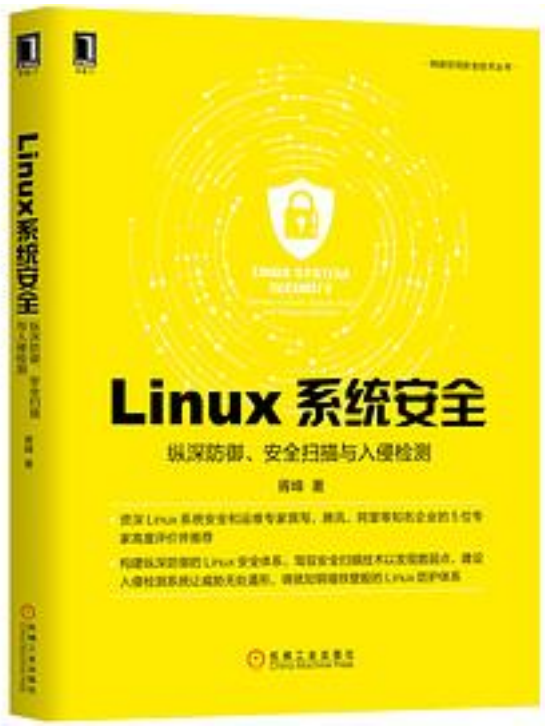
Linux系统安全：纵深防御、安全扫描与入侵检测



Linux系统安全：纵深防御、安全扫描与入侵检测_下载链接1_

著者:胥峰 著

出版者:机械工业出版社

出版时间:2019-7-20

装帧:平装

isbn:9787111632184

这是一部从技术原理、工程实践两个方面系统、深入讲解Linux系统安全的著作，从纵深防御、安全扫描、入侵检测3个维度细致讲解了如何构建一个铜墙铁壁的Linux防护体系。

作者是资深的Linux系统安全专家、运维技术专家，在该领域有13年的从业经验，厚积薄发。本书得到了来自腾讯、阿里等知名企业的多位行业专家的高度评价。全书不仅包含大量工程实践案例，而且对各种核心知识点绘制了方便记忆的思维导图。

全书共14章：

第1章介绍了安全的概念和保障安全的主要原则，引申出了“纵深防御”理念；

第2-3章是纵深防御的第一个关键步骤，即从网络层面对Linux系统进行防护，包含Linux网络防火墙和虚拟专用网络的各个方面；

第4章介绍tcpdump、RawCap、Wiresharklibpcap等网络流量分析工具的技术原理，以及用它们来定位网络安全问题的方法；

第5-7章是纵深防御的第二个关键步骤，即从操作系统层面对Linux系统进行防护，包含用户管理、软件包管理、文件系统管理等核心主题；

第8章是纵深防御的第三个关键步骤，即保障Linux应用的安全，避免应用成为黑客入侵的入口，涵盖网站安全架构、Apache安全、Nginx安全、PHP安全、Tomcat安全、Memcached安全、Redis安全、MySQL安全等话题；

第9章是纵深防御的第四个关键步骤，即确保业务连续性，防御数据被篡改或者数据丢失的风险，讲解了各种场景下的数据备份与恢复；

第10章介绍了nmap、masscan等扫描工具的原理与使用，以及各种开源和商业Web漏洞扫描工具的原理和使用；

第11-13章重点讲解了Linux系统的入侵检测，涉及Linux
Rootkit、病毒木马查杀、日志与审计等主题；

第14章介绍利用威胁情报追踪最新攻击趋势、确定攻击事件性质的方法。

作者介绍:

胥峰

资深运维专家、Linux系统专家和安全技术专家，有13年Linux系统运维和安全经验，在业界颇具威望和影响力。曾就职于盛大游戏，担任架构师，参与多个重大项目的运维和保障，主导运维自动化平台的设计与实施。对DevOps、AIOps等新技术和新思想也有很深的理解。

著有畅销书《Linux运维最佳实践》，同时还翻译了DevOps领域的划时代著作《DevOps：软件架构师行动指南》。

目录: 前言

Linux系统安全：纵深防御、安全扫描与入侵检测_下载链接1_

标签

安全

Linux

计算机

linux

好书，值得一读

信息安全

科技

实用

评论

贵行业出书的门槛也太低了吧

从网络层面、操作系统层面、应用层面和业务连续性4个方面，实现Linux系统的纵深防御。

看完目录决定入手，收到后惊喜地发现每一章还附赠一章思维导图，方便回顾和记忆，这就很贴心，哈哈~

目前生产环境中绝大部分用的都是Linux系统，它的安全性太重要了，这也是个老话题，但是这本书是第一个将这个问题阐述得如此深入、全面的。

这特么评论刷的吧，不适合新人好嘛！！
在这个系列里，和那本数据安全架构的书，刷好评的演员怪不得这么眼熟去你妈的。

没有绝对安全的系统。没有攻不破的系统，只有还没攻破的系统。Linux系统安全是一个庞大的体系，而本书几乎涵盖了保障Linux系统安全的方方面面。这本书既有原理剖析，也有实践指导，是一本该行业从业者或是对Linux安全技术有兴趣者值得读读的书。

胥峰老师在Linux和运维领域大名鼎鼎，书如其人，一个字，牛！

适合新书入门，也适合有一定工作经验的安全从业人员阅读。纵览这本书，让人收获很多。首先它不是简单的说教，也不是长篇大论的理论分析，而是以案例为入口，贴近实战。其次，每章都有清晰的知识脑图，非常有助于读者把握各章内容的关联关系，也非

常方便读者快速记忆核心知识点。作为一个安全工程师，我推荐这本书。

要想拥有一个安全的Linux系统，感觉看这本书足够了，知识点非常全面，几乎面面俱到。

这本书，结构完整体系化，内容详实且深入浅出，非常赞的一本书。

拿到书后，如饥似渴的读了起来。内容写的很好，从安全的用户管理到软件管理、Masscan/Nmap扫描工具的使用、开源入侵检测工具OSSEC的部署安全，非常详尽。希望这本书助我早日成为Linux安全大牛。

胥峰大神的新书，是一定要来支持一下的，他的个人品牌就是内容质量的保证。

难得有书能系统详细的介绍Linux系统安全，填补了这项空白。

书评

Linux系统安全：纵深防御、安全扫描与入侵检测_下载链接1_