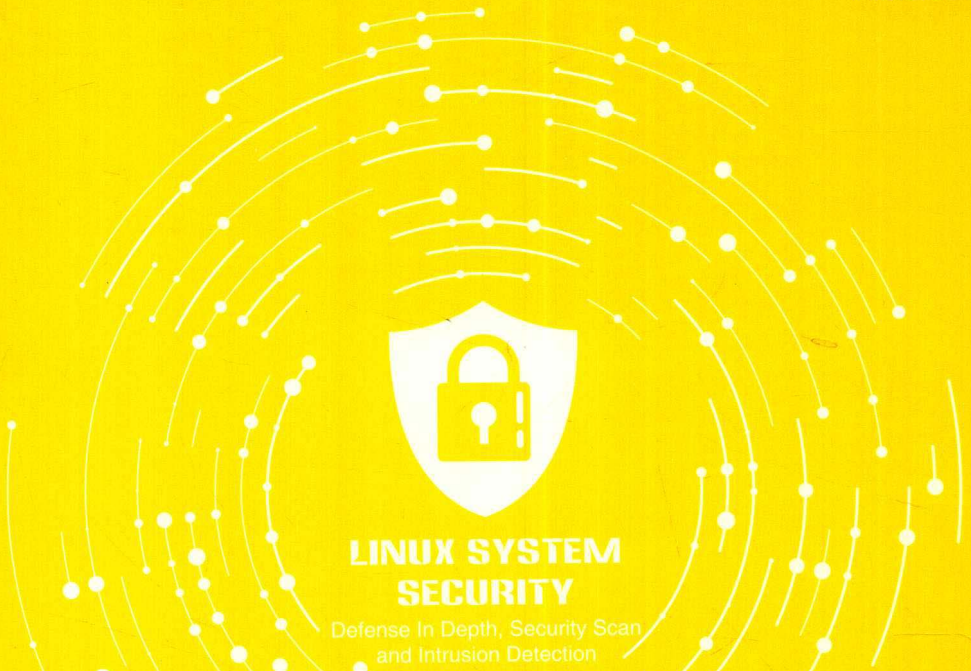
HZ BOOKS
华章IT

· 网络空间安全技术丛书 ·



Linux 系统安全

纵深防御、安全扫描与入侵检测

胥峰 著

- 资深 Linux 系统安全和运维专家撰写，腾讯、阿里等知名企业的 5 位专家高度评价并推荐
- 构建纵深防御的 Linux 安全体系，驾驭安全扫描技术以发现脆弱点，建设入侵检测系统让威胁无处遁形，铸就如铜墙铁壁般的 Linux 防护体系

机械工业出版社
China Machine Press

· 网络空间安全技术丛书 ·

Linux 系统安全

纵深防御、安全扫描与入侵检测

LINUX SYSTEM SECURITY

Defense In Depth, Security Scan and Intrusion Detection

胥峰 著

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

Linux 系统安全：纵深防御、安全扫描与入侵检测 / 胥峰著 . —北京：机械工业出版社，2019.7
（网络空间安全技术丛书）

ISBN 978-7-111-63218-4

I. L… II. 胥… III. Linux 操作系统 – 安全技术 IV. TP316.85

中国版本图书馆 CIP 数据核字（2019）第 137821 号

Linux 系统安全：纵深防御、安全扫描与入侵检测

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码：100037）
责任编辑：李　艺　　责任校对：殷　虹
印　　刷：北京诚信伟业印刷有限公司　　版　　次：2019 年 7 月第 1 版第 1 次印刷
开　　本：186mm × 240mm　1/16　　印　　张：18.25
书　　号：ISBN 978-7-111-63218-4　　定　　价：79.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88379426　88361066　　投稿热线：（010）88379604
购书热线：（010）68326294　　读者信箱：hzit@hzbook.com

前　言

为什么要写本书

我国西汉时期著名学者戴圣在其著作《礼记·中庸》中写道，“凡事豫则立，不豫则废。”面对日益严峻的网络安全形势，这句话尤为适用。

全球知名网络安全公司 Gemalto 发布的《数据泄露水平指数》指出，2018 年上半年，全球每天有超过 2500 万条数据遭到入侵或泄露，涉及医疗、信用卡、财务、个人身份信息等。网络威胁事件时时刻刻在发生，黑客攻击手法也趋于复杂和多样。高速的网络连接是一把双刃剑，它在加速了互联网应用的同时，也助长了入侵者的危害能力。面对这样险峻的形势，我们亟需构建自己的网络防御体系，这样才能做到胸有成竹，御敌于千里之外。

Linux 是广受欢迎的互联网基础设施之一，具有开源、免费的特点，并有丰富健康的生态环境和社区支持。正因如此，Linux 也成为黑客攻击的重要目标，因为其承载了大量互联网上不可或缺的基础服务，也是收集、生产、处理、传输和存储有价值数据的实体。保护 Linux 安全的重要性不言而喻。

笔者注意到，虽然市面上有很多以“信息安全”和“网络安全”为主题的书籍，但这些书籍大多聚焦在安全意识、法律法规和一些通用技术上。虽然这些书籍对网络安全建设起到了一定的指导作用，但是它们并不侧重于 Linux 安全，也不强调在保障 Linux 安全上的特定实践。因此，笔者认为有必要写一本侧重于 Linux 安全实践的书籍，真正把安全的规范和指南落实在 Linux 上，构建 Linux 的安全体系。

本书以 Linux 安全为主线，强调实践。实践出真知，因此，笔者也鼓励读者在阅读

本书的过程中，多多动手在测试机上进行验证，然后把这些技术应用到生产环境中。

本书内容介绍

本书整体上按照纵深防御、安全扫描、入侵检测这 3 个大的方面来组织内容。

第 1 章概要介绍安全的概念和保障安全的主要原则，引申出“纵深防御”理念。

第 2 章、第 3 章是纵深防御的第 1 个关键步骤，是从网络层面对 Linux 系统进行防护。第 4 章介绍了使用相应工具定位网络安全问题的方法。

第 5 ~ 7 章是纵深防御的第 2 个关键步骤，即从操作系统层面对 Linux 系统进行防护。

第 8 章是纵深防御的第 3 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。

第 9 章是纵深防御的第 4 个关键步骤，即确保业务的连续性，降低数据被篡改或者数据丢失的风险。

第 10 章介绍安全扫描的工具及其使用案例。安全并非一蹴而就，它需要按照 PDCA 的顺序不断检查和改进，而安全扫描正是最有效的自我检查途径。通过安全扫描，我们可以发现现有防御手段的不足及新的安全风险，为持续改进提供强有力的、有针对性的指南。

第 11 ~ 13 章介绍入侵检测相关技术和实践，目的是在发生入侵事件后，能够及时发现入侵事件、找到入侵事件遗漏的后门和威胁项、利用日志和审计工具找到黑客的行踪和动作。通过这些技术，我们可以知道黑客是怎么入侵进来的、他做了什么，从而为后续完善防御手段提供支持。

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。

读者对象

本书以广泛适用的信息安全基本原则为指导，聚焦 Linux 安全，强调实战。本书适合的读者对象包括：

- 网络安全工程师
- Linux 运维工程师
- Linux 运维架构师
- Linux 开发工程师
- Web 开发工程师
- 软件架构师
- 大中专院校计算机系学生

勘误和支持

尽管笔者努力确保书中不存在明显的技术错误，但由于技术水平和能力有限，书中可能存在某项技术不适用于读者特定环境的情况，也可能存在纰漏。在此，笔者恳请读者不吝指正。反馈专属邮箱：xufengnju@163.com。

本书中所有已发现的错误，除了在下一次印刷中修正以外，还会通过微信公众号“运维技术实践”（yunweijishushijian）发布。

为了更好地服务读者，笔者建立了本书的专属支持 QQ 群（434242482）。有兴趣的读者可以加入该群，就本书的内容进行探讨。

致谢

写作的过程就像一场长跑，在这个跑道上，我收获了无数的鼓励和支持。

在此，我首先感谢机械工业出版社华章公司的杨福川老师和李艺老师。杨福川老师是出版界的资深人士，他出版了一系列高质量、广受赞誉的 IT 类书籍。杨福川老师协

助我完成了本书的选题并确定了基本内容和组织结构。李艺老师是一位专业、尽职、高效的编辑，她多次就本书提出非常有建设性的建议。

在长达数月的写作过程中，我的太太承担了全部的家庭责任，她使得我能持久安心地完成本书的写作。感谢她！我的女儿今年 5 岁了，活泼灵巧。感谢她成为我生命中的一部分，鼓励我努力前行！

胥峰

目　录

第1章

Linux系统安全概述

著名网站技术调查公司W3Techs（官方网站：https://w3techs.com）于2018年11月17日发布的调查报告[⊖]中指出，Linux在网站服务器操作系统中使用比例高达37.2%。除了被广泛使用在网站平台上以外，Linux也常常被作为FTP服务器、电子邮件服务器、域名解析服务器和大数据分析服务器等而部署在互联网上。Linux作为互联网基础设施的一个重要组成部分，保障其安全的重要性不言而喻。虽然Linux是一款被大量部署的优秀的开源操作系统，但是这并不意味着不需要关注其安全性。在互联网上，有许许多多针对Linux系统的攻击。例如，中国国家计算机病毒应急处理中心（官方网站：http://www.cverc.org.cn）在《病毒预报 第七百六十九期》[⊜]中指出："通过对互联网的监测，发现了一款旨在感染Linux设备的加密货币挖矿恶意程序Linux.BtcMine.174。该恶意程序在不经过设备所有者同意的情况下使用CPU或GPU资源来进行隐蔽的加密货币挖掘操作。"

如果缺乏严密细致的防御措施、积极主动的安全扫描、行之有效的入侵检测系统、切实到位的安全管理制度和流程保障，那么Linux系统很容易被黑客入侵或利用，而保障业务和数据安全也将成为一句空话。

本章概览性地介绍信息安全和系统安全的概念、常见的威胁分析模型和保障安全的主要原则。对于从全局上把握Linux系统安全来说，这些知识是不可或缺的，它们是构建完整Linux系统安全体系的指南，引导着本书后续章节内容。

⊖ https://w3techs.com/technologies/comparison/os-linux,os-windows，访问日期：2018年11月17日。

⊜ http://www.cverc.org.cn/yubao/yubao_769.htm，访问日期：2019年1月5日。

1.1　什么是安全

1500 多年前，由从梵文译成汉文的《百喻经 · 愿为王剃须喻》中讲述了亲信救王的故事。故事中写道："昔者有王，有一亲信，于军阵中，殁命救王，使得安全。"这里的安全指的就是"平安、不受威胁"。

同样，笔者认为，安全是指一种状态，在这种状态下，某种对象或者对象的某种属性是不受威胁的。例如，《中华人民共和国国家安全法》第二条对国家安全的定义是："国家政权、主权、统一和领土完整、人民福祉、经济社会可持续发展和国家其他重大利益相对处于没有危险和不受内外威胁的状态，以及保障持续安全状态的能力。"《中华人民共和国网络安全法》第五条中指出，网络安全的目的之一就是"保护关键信息基础设施免受攻击、侵入、干扰和破坏"，也就是保护关键信息基础设施不受威胁。

1.1.1　什么是信息安全

对于什么是信息安全（Information Security），不同的组织和个人可能有不同的定义。

ISO/IEC、美国国家安全系统委员会和国际信息系统审计协会对信息安全的定义是被大部分信息安全从业人员所认可并支持的。《 ISO/IEC 27001:2005 信息安全管理体系规范与使用指南》中对信息安全的定义是："保护信息的机密性（Confidentiality）、完整性（Integrity）、可用性（Availability）及其他属性，如真实性、可确认性、不可否认性和可靠性。"

美国国家安全系统委员会（Committee on National Security Systems，CNSS）在《 Committee on National Security Systems: CNSS Instruction No. 4009》[⊖]对信息安全的定义是："为了保障机密性、完整性和可用性而保护信息和信息系统，以防止未授权的访问、使用、泄露、中断、修改或者破坏。"

国际信息系统审计协会（Information Systems Audit and Control Association，ISACA）

⊖ https://www.hsdl.org/?abstract&did=7447，访问日期：2018 年 11 月 28 日。

对信息安全的定义是：“在企业组织内，信息被保护，以防止被泄露给未授权用户（机密性）、防止非恰当的修改（完整性）、防止在需要的时候无法访问（可用性）。”

通过以上这 3 个定义我们可以看出，保障信息安全的最重要目的是保护信息的机密性、完整性和可用性这 3 个属性。

- 机密性：信息仅仅能够被已授权的个人、组织、系统和流程访问。例如，个人的银行账户交易流水和余额信息，除了账户持有人、经账户持有人授权的第三方组织、依相关法律法规规定有查询权限的组织以外，不应该被任何其他实体获取到。另外，商业组织的客户联系信息往往也具有较高的价值，也需要保护其机密性。在某些对安全要求较高的行业，甚至特别强调了对机密性的保障。例如，在《支付卡行业数据安全标准 3.2.1 版本（Payment Card Industry Data Security Standard, Version 3.2.1）》[⊖] 3.2.2 条中明确指出，在授权完成后，不能在日志、数据库等位置存储信用卡验证码（CVV2、CVC2、CID、CAV2 等）。这是一个强调信用卡验证码机密性的例子。
- 完整性：保护信息的一致性（Consistency）、准确性（Accuracy）和可信赖性（Trustworthiness）。例如，A 公司向 B 公司提供的数据报告是通过电子邮件附件的形式来传输的，那么 A 公司就需要和 B 公司预先确定一种机制，来检查和确认 B 公司收到的电子邮件附件确实与 A 公司发送的一模一样，是未被在传输过程中篡改的。
- 可用性：当需要访问的时候，信息可以提供给合法授权用户访问。没有了可用性的保障，信息的价值就难以持续体现出来。

在学习信息安全的机密性、完整性和可用性这 3 个属性时，我们可以使用信息安全的 C.I.A 金三角帮助记忆，如图 1-1 所示。

在考虑信息安全的时候，必须把保障信息的机密性、完整性、可用性作为最重要目标，才能建立完善和有效的保护机制，避免顾此失彼。例如，华为公司 2019 年一号文《全面提升软件工程能力与实践，打造可信的高质量产品——致全体员工的一封信》（电

⊖ https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf，访问日期：2019 年 1 月 5 日。

邮讲话【2019】001 号 签发人：任正非）[⊖]指出："公司已经明确，把网络安全和隐私保护作为公司的最高纲领。"其同时指出，"安全性（Security）"的要求就是"产品有良好的抗攻击能力，保护业务和数据的机密性、完整性和可用性"。

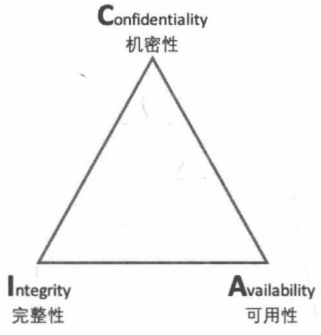


图 1-1　信息安全的 C.I.A 金三角记忆图

1.1.2　信息安全的木桶原理

一般来说，信息安全的攻击和防护是严重不对称的。相对来说，攻击成功很容易，防护成功却极为困难。信息安全水平的高低遵循木桶原理（Bucket effect），如图 1-2 所示。

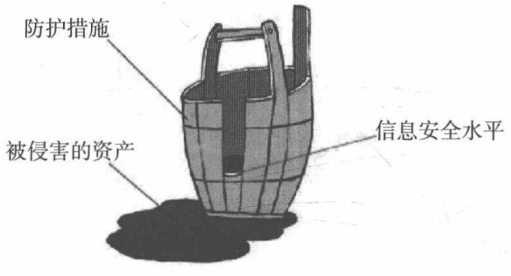


图 1-2　信息安全的木桶原理

如图 1-2 所示，虽然有多种多样的防护措施，但是信息安全水平的高低，却取决于防护最薄弱的环节。木桶原理体现了安全体系建设中对整体性原则的要求。整体性原则要求我们从宏观的、整体的角度出发，系统地建设信息安全体系，一方面，全面构架信

⊖ http://xinsheng.huawei.com/cn/index.php?app=forum&mod=Detail&act=index&id=4134815，访问日期：2019 年 1 月 5 日。

息安全技术体系，覆盖从通信和网络安全、主机系统安全到数据和应用安全各个层面；另一方面，还要建立全面有效的安全管理体系和运行保障体系，使得安全技术体系发挥最佳的保障效果。

1.1.3　Linux 系统安全与信息安全的关系

1.1.1 节介绍了信息安全的概念，那么，本书的主题“Linux 系统安全”与信息安全是什么关系呢？

首先，我们需要认识到，只有保障了 Linux 系统安全，才能保障依赖于其提供服务的信息安全。信息是有生命周期的，从其产生、收集、处理、传输、分析到销毁或者存档，每个阶段都可能有大量的设备、平台、应用介入。而为这些设备、平台、应用提供底层支持的，往往有大量的 Linux 系统（包括服务器和嵌入式设备等），其为信息的整个生命周期提供源源不断的动力支撑。

其次，我们也需要认识到，保障 Linux 系统安全是手段，保障信息安全是目的。如果一个 Linux 系统上没有存储任何有价值的信息，不生产或者传输有价值的信息，不处理和分析有价值的信息，那么这个系统也就失去了保护的价值。对 Linux 系统安全的关注，实际上是对真正有价值的信息的关注。

1.2　威胁分析模型

与安全相对应的是威胁。我们要保障安全，就需要了解威胁是什么。

1.2.1　STRIDE 模型

微软的 STRIDE 模型是常用的威胁模型之一。STRIDE 这 6 个字母分别代表身份欺骗（Spoofing identity）、篡改数据（Tampering with data）、否认性（Repudiation）、信息泄露（Information disclosure）、拒绝服务（Denial of service）、提权（Elevation of privilege）。

STRIDE 模型针对的属性、定义和例子参考如表 1-1 所示。