信息科学与技术丛书

李晨光 编著

UNIX/Linux 网络日志分析与流量监控

- 重量级的 UNIX/Linux 平台日志分析与攻防取证教程
- 详解日志分析与日志挖掘技术、方法、流程
- 业界专家亲历的安全运维实战回放
- 权威的 OSSIM 开源安全信息平台应用案例
- 将枯燥的技术完美融入生动故事中

机械工业出版社
CHINA MACHINE PRESS

信息科学与技术丛书

UNIX/Linux 网络日志分析与流量监控

李晨光　编著

机械工业出版社

本书以开源软件为基础，全面介绍了 UNIX/Linux 安全运维的各方面知识。第一篇从 UNIX/Linux 系统日志、Apache 等各类应用日志的格式和收集方法讲起，内容涵盖异构网络系统日志收集和分析工具使用的多个方面；第二篇列举了二十多个常见网络故障案例，每个案例完整地介绍了故障的背景、发生、发展，以及最终的故障排除过程。其目的在于维护网络安全，通过开源工具的灵活运用，来解决运维实战工作中的各种复杂的故障；第三篇重点讲述了网络流量收集监控技术与 OSSIM 在异常流量监测中的应用。

本书使用了大量开源工具解决方案，是运维工程师、网络安全从业人员不可多得的参考资料。

图书在版编目（CIP）数据

UNIX/Linux 网络日志分析与流量监控 / 李晨光编著. —北京：机械工业出版社，2014.12
（信息科学与技术丛书）
ISBN 978-7-111-47961-1

Ⅰ. ①U… Ⅱ. ①李… Ⅲ. ①UNIX 操作系统②Linux 操作系统
Ⅳ. ①TP316.8

中国版本图书馆 CIP 数据核字（2014）第 213054 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
策划编辑：车 忱
责任编辑：车 忱 责任校对：张艳霞
责任印制：乔 宇

保定市中画美凯印刷有限公司印刷

2015 年 1 月第 1 版 · 第 1 次印刷
184mm×260mm · 29.5 印张 · 730 千字
0001—3000 册
标准书号：ISBN 978-7-111-47961-1
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

电话服务	网络服务
社服务中心：（010）88361066	教 材 网：http://www.cmpedu.com
销 售 一 部：（010）68326294	机工官网：http://www.cmpbook.com
销 售 二 部：（010）88379649	机工官博：http://weibo.com/cmp1952
读者购书热线：（010）88379203	封面无防伪标均为盗版

出 版 说 明

随着信息科学与技术的迅速发展，人类每时每刻都会面对层出不穷的新技术和新概念。毫无疑问，在节奏越来越快的工作和生活中，人们需要通过阅读和学习大量信息丰富、具备实践指导意义的图书来获取新知识和新技能，从而不断提高自身素质，紧跟信息化时代发展的步伐。

众所周知，在计算机硬件方面，高性价比的解决方案和新型技术的应用一直备受青睐；在软件技术方面，随着计算机软件的规模和复杂性与日俱增，软件技术不断地受到挑战，人们一直在为寻求更先进的软件技术而奋斗不止。目前，计算机和互联网在社会生活中日益普及，掌握计算机网络技术和理论已成为大众的文化需求。由于信息科学与技术在电工、电子、通信、工业控制、智能建筑、工业产品设计与制造等专业领域中已经得到充分、广泛的应用，所以这些专业领域中的研究人员和工程技术人员越来越迫切需要汲取自身领域信息化所带来的新理念和新方法。

针对人们了解和掌握新知识、新技能的热切期待，以及由此促成的人们对语言简洁、内容充实、融合实践经验的图书迫切需要的现状，机械工业出版社适时推出了“信息科学与技术丛书”。这套丛书涉及计算机软件、硬件、网络和工程应用等内容，注重理论与实践的结合，内容实用、层次分明、语言流畅，是信息科学与技术领域专业人员不可或缺的参考书。

目前，信息科学与技术的发展可谓一日千里，机械工业出版社欢迎从事信息技术方面工作的科研人员、工程技术人员积极参与我们的工作，为推进我国的信息化建设做出贡献。

机械工业出版社

媒 体 推 荐

日志分析是系统管理员的基本技能。UNIX/Linux 系统提供了强大的日志系统，为管理员查找和发现问题提供了强有力的支持。本书以讲故事的形式，将作者的亲身实战经历融入其中，仿佛福尔摩斯在向华生讲述整个案情的来龙去脉，让读者在跟随作者分析的过程中，了解 UNIX/Linux 日志分析的窍门。本书语言通俗易懂，结合案例情景，易于实践操作。

更重要的是，系统管理员（包括各类 IT 从业者）通过本书，不仅可以学习到 UNIX/Linux 日志的作用，还可以举一反三，站在更高的角度看待 IT 运维和系统安全。只有整体看待这些问题，才能增加系统的稳定性和安全性，将系统管理员从日常事务中解脱出来。

——吴玉征　51CTO 副主编（原〈计算机世界〉报副总编）

本书作者李晨光先生是 51CTO 专家博主，他的文章深受技术同行关注。作者在 2011～2013 年度中国 IT 博客大赛中被评为“十大杰出 IT 博客”，一个如此优秀的博主写的书肯定值得一看。此书详细介绍了 UNIX/Linux 平台下日志分析方法和计算机取证技巧，并以讲故事的形式，介绍日志分析的全过程，其最大亮点是将 UNIX/Linux 系统中枯燥的技术问题，通过生动案例展现出来，每个案例读完后都能让系统管理员们有所收获。读完这本书你一定不会后悔。

——曹亚莉　51CTO 博客总编、51CTO 学院高级运营经理

李晨光老师是 ChinaUnix 专家博主，在 UNIX/Linux 领域研究多年，对日志分析技术有独到见解。这本《UNIX/Linux 网络日志分析与流量监控》是业界第一本基于 UNIX/Linux 环境，讲解应用系统日志收集、分析方法的专著，是李老师多年沉淀的技术结晶。书中采用大量鲜活的案例，生动地展示了系统漏洞防范、恶意代码分析、DoS 分析、恶意流量过滤等安全防护技术，深入分析了诸多系统管理员的错误维护方法及误区，对安全工作者有很好的参考价值。如果你对网络安全、日志分析感兴趣，我们强烈推荐此书。

——ChinaUnix 技术社区

运维人员都很清楚，非常枯燥又不得不做的事情就是服务器日志文件分析和流量监控。尽管现在有很多相关工具和软件，但真正将它们与自己的实际工作相结合时，往往力不从心。这本《UNIX/Linux 网络日志分析与流量监控》以案例驱动的形式从 UNIX/Linux 系统

的原始日志（Raw Log）采集、分析到日志审计与取证环节都进行了详细的介绍和说明，内容非常丰富，中间还穿插了很多小故事，毫不枯燥，让您在轻松的阅读环境中提升自己的日志分析技能。如果是运维人员或想成为运维人员，您值得拥有！

——ITPUB 技术社区

随着网络威胁的日益严峻，信息安全问题受到越来越多的用户关注。而针对 UNIX/Linux 系统的安全探讨，李晨光老师的这本《UNIX/Linux 网络日志分析与流量监控》显然是非常不错的选择，本书通过一个个生动的案例将 UNIX/Linux 系统下的安全问题进行了深入浅出的剖析，让你可以更好地消化其中的方法和技术，非常值得一读。

——董建伟 IT168 安全频道主编

前　言

本书从 UNIX/Linux 系统的原始日志（Raw Log）采集与分析讲起，逐步深入到日志审计与计算机取证环节。书中提供了多个案例，每个案例都以一种生动的记事手法讲述了网络遭到入侵之后，管理人员开展系统取证和恢复的过程，案例分析手法带有故事情节，使读者身临其境地检验自己的应急响应和计算机取证能力。

本书使用的案例都是作者从系统维护和取证工作中总结、筛选出来的，这些内容对提高网络维护水平和事件分析能力有重要的参考价值。如果你关注网络安全，那么书中的案例一定会引起你的共鸣。本书适合有一定经验的 UNIX/Linux 系统管理员和信息安全人士参考。

1. 为什么写这本书

国内已出版了不少网络攻防等安全方面的书籍，其中多数是以 Windows 平台为基础。但互联网应用服务器大多架构在 UNIX/Linux 系统之上，读者迫切需要了解有关这些系统的安全案例。所以我决心写一本基于 UNIX/Linux 的书，从一个白帽的视角，为大家讲述企业网中 UNIX/Linux 系统在面临各种网络威胁时，如何通过日志信息查找问题的蛛丝马迹，修复网络漏洞，构建安全的网络环境。

2. 本书特点与结构

书中案例覆盖了如今网络应用中典型的攻击类型，例如 DDoS、恶意代码、缓冲区溢出、Web 应用攻击、IP 碎片攻击、中间人攻击、无线网攻击及 SQL 注入攻击等内容。每段故事首先描述一起安全事件。然后由管理员进行现场勘查，收集各种信息（包括日志文件、拓扑图和设备配置文件），再对各种安全事件报警信息进行交叉关联分析，并引导读者自己分析入侵原因，将读者带入案例中。最后作者给出入侵过程的来龙去脉，在每个案例结尾提出针对这类攻击的防范手段和补救措施，重点在于告诉读者如何进行系统和网络取证，查找并修复各种漏洞，从而进行有效防御。

全书共有 14 章，可分为三篇。

第一篇日志分析基础（第 1～3 章），是全书的基础，对于 IT 运维人员尤为重要，系统地总结了 UNIX/Linux 系统及各种网络应用日志的特征、分布位置以及各字段的作用，包括 Apache 日志、FTP 日志、Squid 日志、NFS 日志、Samba 日志、iptables 日志、DNS 日志、DHCP 日志、邮件系统日志以及各种网络设备日志，还首次提出了可视化日志分析的实现技术，首次曝光了计算机系统在司法取证当中所使用的思路、方法、技术和工具，这为读者有效记录日志、分析日志提供了扎实的基础，解决了读者在日志分析时遇到的“查什么”、“怎么查”的难题。最后讲解了日志采集的实现原理和技术方法，包括开源和商业的日志分析系统的搭建过程。

第二篇日志分析实战（第 4～12 章），讲述了根据作者亲身经历改编的一些小故事，再现了作者当年遇到的各种网络入侵事件的发生、发展和处理方法、预防措施等内容，用一个

个网络运维路上遇到的“血淋淋”的教训来告诫大家，如果不升级补丁会怎么样，如果不进行系统安全加固又会遇到什么后果。这些案例包括 Web 网站崩溃、DNS 故障、遭遇 DoS 攻击、Solaris 安插后门、遭遇溢出攻击、rootkit 攻击、蠕虫攻击、数据库被 SQL 注入、服务器沦为跳板、IP 碎片攻击等。

第三篇网络流量与日志监控（第 13、14 章），用大量实例讲解流量监控原理与方法，例如开源软件 Xplico 的应用技巧，NetFlow 在异常流量中的应用。还介绍了用开源的 OSSIM 安全系统建立网络日志流量监控网络。

本书从网络安全人员的视角展现了网络入侵发生时，当你面临千头万绪的线索时如何从中挖掘关键问题，并最终得以解决。书中案例采用独创的情景式描述，通过一个个鲜活的 IT 场景，反映了 IT 从业者在工作中遇到的种种难题。案例中通过互动提问和开放式的回答，使读者不知不觉中掌握一些重要的网络安全知识和实用的技术方案。

本书案例中的 IP 地址、域名信息均为虚构，而解决措施涉及的下载网站以及各种信息查询网站是真实的，具有较高参考价值。书中有大量系统日志,这些日志是网络故障取证处理时的重要证据，由于涉及保密问题，所有日志均做过技术处理。

由于时间紧，能力有限，书中不当之处在所难免，还请各位读者到我的博客多多指正。

3. 本书实验环境

本书选取的 UNIX 平台为 Solaris 和 FreeBSD，Linux 平台主要为 Red Hat 和 Debian Linux。涉及取证调查工具盘是 Deft 8.2 和 Back Track5。在 http://chenguang.blog.51cto.com（作者的博客）提供了 DEFT-vmware、BT5-vmware、OSSIM-vmware 虚拟机，可供读者下载学习研究。

4. 致谢

首先感谢我的父母多年来的养育之恩和关心呵护。感谢我在各个求学阶段的老师。尤其要感谢我的妻子，有了她精心的照顾，我才能全身心地投入到创作当中，没有她的支持和鼓励，我无法持之以恒地完成本书。最后要感谢机械工业出版社的车忱编辑，为了提升本书的质量，他花费了大量心血。

李晨光

2014 年 7 月

目　录

第二篇 日志分析实战