51CTO学院丛书

异步图书
www.epubit.com

开源安全运维平台

OSSIM疑难解析

51CTO 学院策划
李晨光 著

提高篇

中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

51CTO学院丛书

异步图书
www.epubit.com

开源安全运维平台

OSSIM疑难解析

51CTO 学院策划
李晨光 著

提高篇

人民邮电出版社
北京

图书在版编目（CIP）数据

开源安全运维平台OSSIM疑难解析. 提高篇 / 李晨光著. -- 北京 : 人民邮电出版社, 2019.9
（51CTO学院丛书）
ISBN 978-7-115-50647-4

Ⅰ. ①开… Ⅱ. ①李… Ⅲ. ①Linux操作系统－安全技术 Ⅳ. ①TP316.85

中国版本图书馆CIP数据核字(2019)第025981号

内 容 提 要

OSSIM（Open Source Security Information Management，开源安全信息管理）系统是一个非常流行和完整的开源安全架构体系，通过将开源产品进行集成，从而提供一种能实现安全监控功能的基础平台。

本书精选了作者在OSSIM日常运维操作中遇到的许多疑难杂症，并给出了相应的解决方案。本书共分为12章，内容包括入侵检测Snort与Suricata，基于主机的入侵检测——OSSEC，漏洞扫描OpenVAS，Memcache、RabbitMQ与Redis协同工作，日志采集与分析，关联分析技术，资产管理，网络流量与主机高可用监控，NetFlow流量分析，OSSIM前端汉化技巧，压力测试及性能监控，数据包抓包分析技巧等。

本书非常适合具有一定SIEM（Security Information and Event Management，安全信息和事件管理）系统实施经验的技术经理或中高级运维工程师阅读，还可以作为开源技术研究人员、网络安全管理人员的参考资料。

◆ 著　　李晨光
责任编辑　傅道坤
责任印制　焦志炜

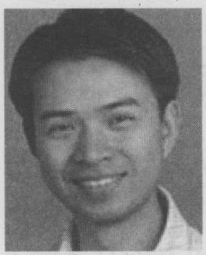
◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路11号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京圣夫亚美印刷有限公司印刷

◆ 开本：800×100　1/16
印张：22.75
字数：494千字　　2019年9月第1版
印数：1－2 000册　　2019年9月北京第1次印刷

定价：89.00元

读者服务热线：(010)81055410　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京东工商广登字20170147号

作者简介



李晨光，OSSIM 布道师、资深网络架构师、UNIX/Linux 系统安全专家、中国计算机学会高级会员。他写作的《Linux 企业应用案例精解》《UNIX/Linux 网络日志分析与流量监控》《开源安全运维平台 OSSIM 最佳实践》在图书市场上具有相当抢眼的表现与上佳口碑，且中文繁体字版本也被输出到中国台湾。

李晨光先生还是 51CTO、ChinaUnix、OSChina 等社区的专家博主，撰写的技术博文被国内各大 IT 技术社区广泛转载，还曾多次受邀在国内系统架构师大会和网络信息安全大会上发表技术演讲。

前 言

写作本书的目的

目前，OSSIM 在中国移动、中国电信、中国石油、华为等大型企业内得到应用推广，这些企业在安全运营中心（SOC）的基础上组建了 OSSIM 运维和二次开发团队，但图书市场缺乏专门讲解 OSSIM 运维和开发的书籍。为了解答 OSSIM 运维工程师在工作中遇见的疑难问题，本书应运而生。

本书借助作者在 OSSIM 领域长达 10 年的开发应用实践经验，以大量实际问题为线索，阐述了基于插件收集的日志并实现标准化、安全事件规范化分类、关联分析的精髓。书中给出的参考答案有利于读者深入理解各种问题，让读者主动思考问题，从而避免死读书。书中展示的所有问题原型均来自大型企业中复杂的生产环境，给出的参考答案也是作者认为比较好的一种处理方案。

本书编写形式新颖，表达方式独特，图文并茂，通俗易懂，有很强的实用性。读者在学习和阅读的过程中可以针对自己感兴趣的问题得到及时、明确的解答。在满足碎片化阅读的同时，本书还通过近百道课后习题加深读者对 OSSIM 系统的理解。

本书主要内容

本书介绍了开源 OSSIM 系统安装部署以及运维管理的若干疑难问题，共分 12 章。

- **第 1 章，入侵检测 Snort 与 Suricata**，讲解入侵检测系统 Snort 和 Suricata 在 OSSIM 系统中的应用问题。
- **第 2 章，基于主机的入侵检测——OSSEC**，讲解在 HIDS-OSSEC 部署过程中常见的故障并进行解答。
- **第 3 章，漏洞扫描 OpenVAS**，讲解在漏洞扫描 OpenVAS 服务器安装过程中遇到的疑难问题。
- **第 4 章，Memcache、RabbitMQ 与 Redis 协同工作**，讲解 Memcache、RabbitMQ 和 Redis 等缓存和中间件系统在系统维护与管理中遇到的配置难点及疑难问题。

- **第 5 章，日志采集与分析**，讲解利用 OSSIM 进行日志采集和分析的问题。
- **第 6 章，关联分析技术**，讲解 OSSIM 关联分析技术问题。
- **第 7 章，资产管理**，讲解利用 OSSIM 进行资产管理的问题。
- **第 8 章，网络流量与主机高可用监控**，讲解利用 Ntop 和 Nagios 进行流量管理的问题。
- **第 9 章，NetFlow 流量分析**，讲解利用 NetFlow 为 OSSIM 进行流量分析的问题。
- **第 10 章，OSSIM 前端汉化技巧**，讲解 OSSIM 前端汉化技巧。
- **第 11 章，压力测试及性能监控**，讲解利用开源工具对 OSSIM 进行性能测试以及调优的技巧问题。
- **第 12 章，数据抓包分析技巧**，讲解抓包分析技术。

本书读者对象

本书精选了作者在 OSSIM 日常运维操作中总结的 300 多个疑难问题，是 OSSIM 运维工程师故障速查手册，专门针对 OSSIM 故障解答而编写。本书适合具有一定 SIEM 系统实施经验的技术经理或中高级运维工程师阅读，还可作为信息安全专家和相关领域研究人员的参考书，也可作为高等学校网络工程和信息安全专业的教材。

本书约定

关于版本

在本书中，软件的安装环境为 Debian Linux 8.0。在安装其他软件时，必须符合该版本要求。

关于菜单的描述

OSSIM 的前台界面复杂，书中经常会用一串带箭头的单词表达菜单的路径，例如 Web UI 中的 Dashboards→Overview→Executive，表示 Web 界面下鼠标依次单击 Dashboards、Overview，最后到达 Executive 仪表盘。

路径问题

除非特别说明，本书所涉及路径均指在 OSSIM 系统下的路径，而不是其他 Linux 发行版。终端控制台是指通过 root 登录系统，然后输入 ossim-setup 启动 OSSIM 终端控制台的界面。

在终端控制台下，选择 Jailbreak 系统菜单就能进入 root shell，登录日志会保存在文件 /var/log/ossim/root_access.log 中。

SIEM 事件分析控制台

SIEM 控制台是指通过 Web UI 进入系统，在菜单 Analysis→SIEM 下的界面。

关于 OSSIM 服务器端与传感器端的约定

本书讲述的 OSSIM 服务器端均指通过 AlienVault USM 安装的系统，包括 OSSIM 四大组件，传感器端是通过 AlienVault Sensor 安装的系统。

关于地图显示问题

所有地图信息均来自谷歌地图，大家在做实验前确保已连上谷歌地图，而且使用系统中的 OTX 时也需要能连接到谷歌地图。

浏览器约定

OSSIM Web UI 适合采用 Safari 7.0、Google Chrome 44.0、IE 10.0 以上的浏览器访问。

实验环境下载

本书涉及的软件较多，其中一些重要的软件可到异步社区的本书页面中统一获取。

学习之路中如何面对失败

与其他 Linux 系统一样，在学习 OSSIM 的过程中也会出现各种问题和故障。由于网上能直接找到的资料有限，所以很多新手都担心出现问题，在面对问题时都很局促，特别是当一个个问题接踵而来时会显得无可奈何。

学习 OSSIM 可以充分暴露你的“知识短板”，这体现在编程语言、数据库、操作系统、TCP/IP、网络安全的各个方面，不过通过解决在 OSSIM 里遇到的问题，就会逐步弥补这些短板。学习就是一个发现问题与解决问题的过程，只要掌握了 OSSIM 的体系结构和运行原理，很多问题都可以迎刃而解。当然前提是我们已经具备了下面所列的这些扎实的基本功：

- 有一定的英文水平；
- 了解网络原理尤其是 TCP/IP 的内容；
- Debian Linux 系统和网络管理知识；
- MySQL 数据库的基本操作；
- 服务器、网络设备运维基础；
- 系统攻击与应急响应相关的技能；
- IDS 部署和 SIEM/SOC 应用基础。

要成为 OSSIM 系统运维人员，面对问题时头脑中必须有一个清晰、明确的故障解决思路，一般有以下 5 个步骤。

- 从报错提示挖掘幕后问题：OSSIM 在 Web UI 中报错，主要内容都显示在屏幕上，只要看懂错误提示（前提是能读懂英文），就基本能猜出发生问题的几种可能性。

- 查看日志文件：Web 前台报错，在后台日志会有详细的错误日志。系统日志在文件/var/log 中，OSSIM 日志在/var/log/ossim 或/var/log/alienvault/中，结合两个目录下的日志就有可能发现问题。
- 定位问题：这个过程相对复杂，经过 Web 里的提示和挖掘的日志就能基本推测出现问题的几种途径。
- 解决问题：抓住最有可能的途径进行排除，最后就能解决真正的问题。
- 不要恋战：有些人特别执着，有着不解决问题誓不罢休的架势。遇到一些 OSSIM 故障问题，若在尝试各种思路后依然无法得到自己想要的结果，这时就不要再恋战了，而是跳过这个问题，继续前进。通过休息等方式来疏解一下心中的情绪，没准在过几天的实验结果中会联想到实验失败的教训，进而激发出新的灵感来解决以前的问题。

以上只是解决问题的基本步骤，实验失败是一段充满教育性的成长经历，没有失败积累经验，何谈成功呢？失败次数越多，你对它的理解就越深，离突破性成功就越近。但很多人却不这么看，他们在安装配置 OSSIM 的过程中，接连遇到一两个失败的经历就对这款工具没什么兴趣以至于最后放弃。

在安装阶段遇到的典型问题有下面这些。

- 无法找到硬盘或者网卡驱动。这主要是硬件驱动问题，初学者只要选择 VMware 虚拟机进行安装就能解决。
- 安装过程停滞。在 OpenVAS 解包安装时，界面上出现卡死现象（其实是后台更新脚本时间比较长，在安装界面表现为停滞状态）。很多人在这个环节直接将机器重启，认为自己的操作或者安装文件出了问题，其实只要耐心等待 20 分钟就能过去。
- 系统引导应是短暂的，但有时候却长期停留在引导界面。其实这是假象，只要在控制台上按下 Ctrl+Alt+F3 组合键就会出现命令行登录界面。
- 安装完成，经过长时间的系统引导后，发现无法登录 WebUI。
- 登录 Web UI 后设置的 admin 密码不符合系统的复杂度要求，其实采用 8 位字母数字的组合就能快速解决这个问题。

除此之外，还有路由不通、图形无法显示、抓不到包、采集不到日志等许多故障。无论你是新手还是专家，只要坚持学习 OSSIM，就会不断遇到各种问题。老问题解决了，换个环境，新问题还会不断发生。如果都能逐一化解，那么你的业务能力和分析问题、解决问题的能力会逐步增强。

学习过程中的提问技巧

在系统出现问题时，大家通常会上网寻找答案，比如通过 QQ 群、百度、谷歌或者 AlienVault

社区、Blog 等方式。在这些地方，他们往往将自己的报错信息粘到网上，便坐等答案出现（其实“坐等”“跪求”都无济于事）。

在专家眼里，是否对你提出的技术问题进行解答，很大程度上取决于提问的方式与此问题的难度。一些读者在提问前不深入思考，也不做功课，而是随便提出问题，想利用守株待兔的方式轻易获取问题的答案，这样能取得真经吗？不经历风雨又怎能见到彩虹！

从另一个方面看，专家会觉得你自己不愿意付出，在浪费他们的时间，因此你自然也不会得到想要的结果。专家最喜欢那些真正对问题有兴趣并愿意主动参与解决问题的人，而且只有提出有技术含量的问题，他才会花时间为你回答问题。

提问前的准备工作

作为提问者，必须表现出解决此问题的积极态度，应该提前做些功课，举例如下。

- 善于利用搜索引擎在网络中搜索。在相关技术论坛发帖时要注意，不要在面向高级技术的论坛上发布初级的技术问题，反之亦然。发帖时不要在同一论坛反复发布同一问题，以免被管理员认定为“灌水”。
- OSSIM 帮助系统比较完善，如果善用帮助系统，那么可以解决大部分参数的使用问题。
- 自己检查，反复做实验。
- 尝试阅读 OSSIM 源代码。

问题描述技巧

在描述问题时，请遵循以下技巧。

- 描述症状时不做猜测：明确表达问题的原始状态。
- 按时间顺序描述问题症状：解决问题最有效的线索就是故障出现之前发生的情况。所以，应准确地记录计算机和软件在崩溃前的情况。在使用命令行处理的情况下，对话日志的记录会非常有帮助。如果崩溃的程序有诊断选项，就试着选择能生成排错日志的选项。
- 大段问题的处理：如果你的问题记录很长（如超过 3 段），那么在开头简述问题，然后按时间先后详细描述过程也许更有用。

附件格式及注意事项

有些读者在提问时，喜欢贴一堆日志或者几张图然后发问，前因后果都不讲清楚，就想着获得答案。提问都懒得说清楚，专家也懒得回复。所以，请稍微花一些时间组织语言，把问题说清楚。注意体现文字的准确性和你思考问题的积极性。

最好把问题连同故障截图（提供完整截图）作为附件发给专家，建议使用标准的文件格式发送，以下是参考格式。

- 使用纯文本或者 PDF 格式，也可以使用 doc、RTF 格式。

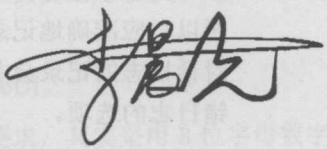
- 发送邮件时如有多个附件，压缩打包后检查附件内容是否能正常打开。
- 发送原始数据，并保持内容一致，例如截屏或者屏幕录像。
- 如果用 Windows 操作系统发送电子邮件，则关闭“引用”功能，以免在邮件中出现乱码。

致谢

首先感谢我的父母多年来的养育之恩；其次感谢在我各个求学阶段给予帮助和支持的老师；最后感谢我的妻子，正因为有了她的精心照顾，我才能全身心地投入到图书创作中。

勘误和支持

由于作者水平有限，书中难免会出现错误和不准确的地方，恳请读者批评指正。如果您有更多宝贵意见，欢迎给我发邮件或者通过我的微信公众号进行反馈。本书的勘误也会通过公众号进行发布。请读者扫描下面的二维码进行关注。



2019 年 7 月

资源与支持

本书由异步社区出品，社区（https://www.epubit.com/）为您提供相关资源和后续服务。

配套资源

本书提供如下资源：

- 本书涉及的部分重要软件。

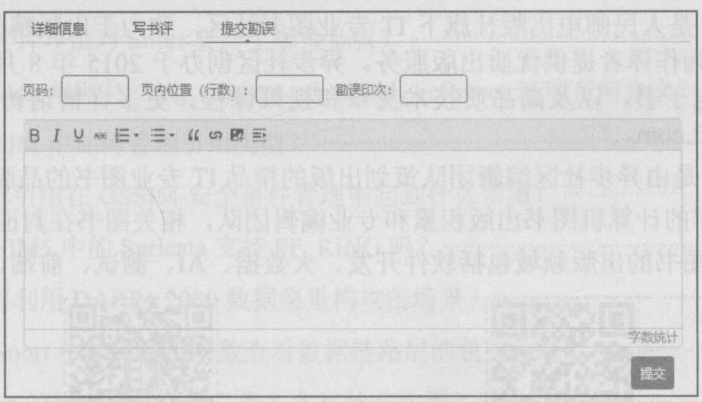
要获得以上配套资源，请在异步社区本书页面中点击 配套资源，跳转到下载界面，按提示进行操作即可。注意：为保证购书读者的权益，该操作会给出相关提示，要求输入提取码进行验证。

如果您是教师，希望获得教学配套资源，请在社区本书页面中直接联系本书的责任编辑。

提交勘误

作者和编辑尽最大努力来确保书中内容的准确性，但难免会存在疏漏。欢迎您将发现的问题反馈给我们，帮助我们提升图书的质量。

当您发现错误时，请登录异步社区，按书名搜索，进入本书页面，点击“提交勘误”，输入勘误信息，点击“提交”按钮即可。本书的作者和编辑会对您提交的勘误进行审核，确认并接受后，您将获赠异步社区的 100 积分。积分可用于在异步社区兑换优惠券、样书或奖品。



扫码关注本书

扫描下方二维码，您将会在异步社区微信服务号中看到本书信息及相关的服务提示。

与我们联系

我们的联系邮箱是 contact@epubit.com.cn。

如果您对本书有任何疑问或建议，请您发邮件给我们，并请在邮件标题中注明本书书名，以便我们更高效地做出反馈。

如果您有兴趣出版图书、录制教学视频，或者参与图书翻译、技术审校等工作，可以发邮件给我们；有意出版图书的作者也可以到异步社区在线提交投稿（直接访问 www.epubit.com/selfpublish/submission 即可）。

如果您是学校、培训机构或企业，想批量购买本书或异步社区出版的其他图书，也可以发邮件给我们。

如果您在网上发现有针对异步社区出品图书的各种形式的盗版行为，包括对图书全部或部分内容的非授权传播，请您将怀疑有侵权行为的链接发邮件给我们。您的这一举动是对作者权益的保护，也是我们持续为您提供有价值的内容的动力之源。

关于异步社区和异步图书

“异步社区”是人民邮电出版社旗下 IT 专业图书社区，致力于出版精品 IT 技术图书和相关学习产品，为作译者提供优质出版服务。异步社区创办于 2015 年 8 月，提供大量精品 IT 技术图书和电子书，以及高品质技术文章和视频课程。更多详情请访问异步社区官网 https://www.epubit.com。

“异步图书”是由异步社区编辑团队策划出版的精品 IT 专业图书的品牌，依托于人民邮电出版社近 30 年的计算机图书出版积累和专业编辑团队，相关图书在封面上印有异步图书的 LOGO。异步图书的出版领域包括软件开发、大数据、AI、测试、前端、网络技术等。

异步社区

微信服务号

目 录