《开源安全运维平台——OSSIM最》

图书基本信息

书名：《开源安全运维平台——OSSIM最佳实践》

13位ISBN编号：9787302423857

出版时间：2016-1-1

作者：李晨光

页数：648

《开源安全运维平台——OSSIM最》

内容概要

在传统的异构网络环境中，运维人员往往利用各种复杂的监管工具来管理网络，由于缺乏一种集成安全运维平台，当遇到故障时总是处于被动“救火”状态，如何将资产管理、流量监控、漏洞管理、入侵监测、合规管理等重要环节，通过开源软件集成到统一的平台中，以实现安全事件关联分析，可从本书介绍的OSSIM 平台中找到答案。本书借助作者在OSSIM 领域长达10 年开发应用实践经验之上，以大量生动实例阐述了基于插件收集日志并实现标准化，安全事件规范化分类，关联分析的精髓，书中为读者展示的所有知识和实例均来自大型企业中复杂的生产环境，并针对各种难题给出解决方案。
全书共分三篇，10 章：第一篇（第1~2 章）主要介绍OSSIM 架构与工作原理、系统规划、实施关键要素和过滤分析SIEM 事件的要领。第二篇（第3~6 章）主要介绍SSIM 所涉及的几个后台数据库，重点强调安全事件分类聚合、提取流程、关联分析算法、Snort 规则分析等技巧。第三篇（第7~10 章）主要介绍日志收集方法和标准化实现思路以及在OSSIM 中用HIDS/NIDS、NetFlow 抓包分析异常流量的方法，深入分析了OpenVAS 架构和脚本分析方法。
本书可以作为开源安全技术研究人员、网络安全管理人员以及高校计算机专业师生学习参考使用。

《开源安全运维平台——OSSIM最》

作者简介

李晨光，毕业于中国科学院研究生院，目前就职于世界500强企业，资深网络架构师、51CTO学院讲师、IBM精英讲师、UNIX/Linux系统安全专家，现任中国计算机学会（CCF）高级会员，曾独著畅销书《Linux企业应用案例精解》、《Linux企业应用案例精解第2版》和《Unix/Linux网络日志分析与流量监控》，均被国内200多家图书馆收藏，经常在国内系统架构师大会、互联网运维与开发者大会和网络信息安全大会上发表技术演讲。

《开源安全运维平台——OSSIM最》

书籍目录

《开源安全运维平台——OSSIM最》

精彩短评

1、一本介绍OSSIM4.8的书，跟我的5.3.6环境有些不同，不过作为入门书还是挺好，比较全面。
2、OSSIM内容丰富，里面有关关联分析规则和安全评估的内容很给力，整个平台基于Web界面操作集中、方便，主要是基于4.8的版本讲的，以后希望能讲讲5.2.x的内容。
3、看目录，还不错。
4、OSSIM很强大，有很多安全功能值得深入再利用。
5、最近在实施一个SIEM系统，遇到日志存储数据库的问题，在网上找了许久，也没有切实可行的方案，直到朋友介绍了这本OSSIM最佳实践，按照书里介绍的思路解决了问题，发散看了看其他内容总的来说里面讲的案例比较使用，项目目前也开始上线，这本书里的内容还需要继续研究下去。
6、讲了一些OSSIM操作和安全运维经验，值得反复阅读。
7、新华书店看到的，价钱虽然有些高，里面介绍OSSIM细节原理比较实用，介绍的ossec,openvas开源工具的使用较详细，便于参考。
8、作为开源安全运营集大成者的开源系统ossim，本书不但讲解了原理、功能，而且详细介绍了组件的安装使用要点，不乏开源软件实践中各种坑的预防。系统架构的sense和server，部署和安装的性能考虑，资产nmap的发现与管理、入侵检测snort、流量分析netflow、监控ngios、包分析wireshark、漏洞扫描和管理opencvs，还有大量集成的实用工具。siem的理念下关联分析、态势感知、预警和报告也说出了开源与商业版的关键区别，规则和报告等知识资产是安全运营的核心，可以基于ossim构建平台，发挥效能需要实践的知识资产库建设。
9、学习了书中介绍的OSSIM关联分析规则，赛选事件很有效。
10、奔着OSSEC、入侵检测和漏洞扫描去的，这本书里讲的集成OSSIM系统很实用，安装配置挺省事的。
11、OSSIM资料不多见，不好找，试读了2章不错，比较受用。
12、OSSIM涉及的原理架构和操作，网络安全测试等内容都有，而且写的很全面，适合像我这样，刚踏入安全圈的工程师，赞！
13、关联分析引擎是OSSIM的核心，在平时的日志分析中筛选事件告警很有用，书中第四章讲了不少关联分析以及规则制定的内容，对我们的安全审计平台开发工作，能借鉴其中的一些内容。
14、几十种开源工具攒在一起的系统，思路不错，没想到还能这样做，安全运维值得看。用一个镜像文件就搞定配置，还是挺方便，就是不支持中文不好。另外sensor在centos上安装不上为什么？
15、从技术开发者角度来说OSSIM流程原理介绍的比较详细，在OSSIM Web UI 上有大量篇幅介绍如何使用OSSIM的功能，并结合网络安全需求如何使用OSSIM，如果再加上源码分析和数据库分析就更好了。
16、OSSIM cookbook!
17、从51CTO读书频道推荐看到的，书的包装不错。半年了，一直在研究OSSIM，公司上线的都是5.3版本，书里讲解的都是4.11的，虽然有些差异，但主要netflow监控和IDS功能和关联检测原理讲解的还是很详细，收获挺多，另外书里截图黑白的还是一些影响阅读体验。
18、OSSIM的系统知识讲的比较详细，干货多。
19、对书中介绍的安全事件关联分析技术感兴趣，讲解的技术比较实用。
20、介绍OSSIM的技术比较全面，实战性强，包含了很多作者的经验在里面，报装不是太好，而且太厚重，不太便于携带。

《开源安全运维平台——OSSIM最》

章节试读

1、《开源安全运维平台——OSSIM最佳实践》的笔记-第75页

OSSIM比一些通过源码包安装的开源工具安装还是要简单多了，直接安装好ISO就能直接使用。只不过在物理服务器上安装有时后会遇到网卡无法识别的现象，要手工安装网卡驱动程序才能驱动起来。识别的硬件不是很多。识别新硬件的能力上这比Centos要差。可能是我对Debian还不怎么熟悉吧。继续看书啦。

《开源安全运维平台——OSSIM最》

版权说明