

《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

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu111.com

《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。

书籍目录

目录

第一篇 基础篇

第1章 OSSIM架构与原理

3

1.1 OSSIM概况

3

1.1.1 从SIM到OSSIM

4

1.1.2 安全信息和事件管理 (SIEM)

5

1.1.3 OSSIM的前世今生

6

1.2 OSSIM架构与组成

13

1.2.1 主要模块的关系

14

1.2.2 安全插件 (Plugins)

15

1.2.3 采集与监控插件的区别

17

1.2.4 检测器 (Detector)

20

1.2.5 代理 (Agent)

20

1.2.6 报警格式的解码

21

1.2.7 OSSIM Agent

22

1.2.8 代理与插件的区别

26

1.2.9 传感器 (Sensor)

26

1.2.10 关联引擎

28

1.2.11 数据库 (Database)

30

1.2.12 Web 框架 (Framework)

31

1.2.13 Ajax创建交互

32

1.2.14 归一化处理

32

1.2.15 标准的安全事件格式

33

1.2.16 OSSIM服务端口

37

1.3 基于插件的日志采集

39	
1.3.1	安全事件分类
39	
1.3.2	采集思路
39	
1.4	Agent事件类型
44	
1.4.1	普通日志举例
45	
1.4.2	plugin_id一对多关系
45	
1.4.3	MAC事件日志举例
47	
1.4.4	操作系统事件日志举例
47	
1.4.5	系统服务事件日志举例
47	
1.5	RRDTool绘图引擎
48	
1.5.1	背景
49	
1.5.2	RRD Tool与关系数据库的不同
49	
1.5.3	RRD绘图流程
49	
1.6	OSSIM工作流程
50	
1.7	缓存与消息队列
50	
1.7.1	缓存系统
50	
1.7.2	消息队列处理
51	
1.7.3	RabbitMQ
53	
1.7.4	选择Key/Value存储
54	
1.7.5	OSSIM下操作Redis
54	
1.7.6	Redis Server配置详解
57	
1.7.7	RabbitMQ、Redis与Memcached监控
58	
1.8	OSSIM 高可用架构
60	
1.8.1	OSSIM高可用实现技术
60	
1.8.2	安装环境
62	

1.8.3 配置本地主机	62
1.8.4 配置远程主机	62
1.8.5 同步数据库	63
1.8.6 同步本地文件	63
1.9 OSSIM防火墙	64
1.9.1 理解Filter机制	64
1.9.2 规则匹配过程	66
1.9.3 iptables规则库管理	67
1.10 OSSIM的计划任务	68
1.10.1 Linux计划任务	68
1.10.2 OSSIM中的计划任务	70
1.11 小结	72
第2章 OSSIM部署与安装	73
2.1 OSSIM安装策略	73
2.1.1 未授权行为	74
2.1.2 传感器位置	75
2.2 分布式OSSIM体系	75
2.2.1 特别应用	76
2.2.2 多IDS系统应用	76
2.3 安装前的准备工作	77
2.3.1 软硬件配备	77
2.3.2 传感器部署	78
2.3.3 分布式OSSIM系统探针布局	80
2.3.4 OSSIM服务器的选择	81
2.3.5 网卡的选择	

82	
2.3.6	手动加载网卡驱动
83	
2.3.7	采用多核还是单核CPU
83	
2.3.8	查找硬件信息
84	
2.3.9	OSSIM USM和Sensor安装模式的区别
84	
2.3.10	OSSIM商业版和免费版比较
86	
2.3.11	OSSIM实施特点
87	
2.3.12	OSSIM管理员分工
88	
2.4	混合服务器/传感器安装模式
88	
2.4.1	安装前的准备工作
88	
2.4.2	开始安装OSSIM
89	
2.4.3	遗忘Web UI登录密码的处理方法
92	
2.5	初始化系统
92	
2.5.1	设置初始页面
93	
2.5.2	OTX——情报交换系统
100	
2.6	VMware ESXi下安装OSSIM注意事项
103	
2.6.1	设置方法
103	
2.6.2	虚拟机下无法找到磁盘的对策
104	
2.7	OSSIM分布式安装实践
104	
2.7.1	基于OpenSSL的安全认证中心
105	
2.7.2	安装步骤
105	
2.7.3	分布式部署（VPN连接）举例
106	
2.7.4	安装多台OSSIM（Sensor）
108	
2.7.5	Sensor重装流程
114	
2.8	添加VPN连接
114	

2.8.1 需求	114
2.8.2 Server端配置 (10.0.0.30)	114
2.8.3 配置Sensor (10.0.0.31)	115
2.9 安装最后阶段	116
2.10 OSSIM安装后续工作	117
2.10.1 时间同步问题	117
2.10.2 系统升级	118
2.10.3 apt-get 常见操作	121
2.10.4 扫描资产	122
2.10.5 通过代理升级系统	122
2.10.6 防火墙设置	124
2.10.7 让控制台支持高分辨率	124
2.10.8 手动修改服务器 IP地址	125
2.10.9 修改系统网关和DNS地址	125
2.10.10 更改默认网络接口	125
2.10.11 消除登录菜单	126
2.10.12 进入OSSIM单用户模式	126
2.10.13 定制系统启动界面	126
2.11 OSSIM启动与停止	127
2.12 安装远程管理工具	129
2.12.1 安装Webmin管理工具	129
2.12.2 安装phpMyAdmin	130
2.12.3 用phpMyAdmin同步功能迁移数据库	132
2.13 分布式系统查看传感器状态	132
2.13.1 设置指示器	

132	
2.13.2	注意事项
134	
2.14	安装桌面环境
135	
2.14.1	安装GNOME环境
135	
2.14.2	安装FVWM环境
135	
2.14.3	安装虚拟机
139	
2.15	自动化配置管理工具Ansible
141	
2.15.1	SSH的核心作用
141	
2.15.2	Ansible配置
143	
2.15.3	Ansible实战
143	
2.15.4	丰富的模块
147	
2.15.5	Ansible与其他配置管理的对比
147	
2.16	SIEM控制台基础
147	
2.16.1	SIEM控制台日志过滤技巧
148	
2.16.2	将重要日志加入到知识库
153	
2.16.3	SIEM中显示不同类别日志
156	
2.16.4	常见搜索信息
158	
2.16.5	仪表盘显示
158	
2.16.6	事件删除与恢复
160	
2.16.7	深入使用SIEM控制台
161	
2.16.8	SIEM事件聚合
164	
2.16.9	SIEM要素
165	
2.16.10	SIEM警报中显示计算机名
172	
2.16.11	SIEM事件保存期限
172	
2.16.12	SIEM数据源与插件的关系
173	

2.16.13 SIEM日志显示中出现0.0.0.0地址的含义

174

2.16.14 无法显示SIEM安全事件时处理方法

174

2.16.15 SIEM数据库恢复

175

2.16.16 EPS的含义

175

2.16.17 常见OSSIM 安装/使用错误

176

2.17 可视化网络攻击报警Alarm分析

178

2.17.1 报警事件的产生

179

2.17.2 报警事件分类

179

2.17.3 五类报警数据包样本下载

184

2.17.4 报警分组

184

2.17.5 识别告警真伪

186

2.17.6 触发OSSIM报警

186

2.18 小结

194

第二篇 提高篇

第3章 OSSIM数据库概述

197

3.1 OSSIM数据库组成

197

3.1.1 MySQL

197

3.1.2 本地访问

198

3.1.3 检查、分析表

200

3.1.4 启用MySQL慢查询记录

201

3.1.5 远程访问

202

3.1.6 MongoDB

203

3.1.7 SQLite

203

3.2 OSSIM数据库分析工具

203

3.2.1 负载模拟方法

204

3.2.2 利用MySQL Workbench工具分析数据库

206

3.3 查看OSSIM数据库表结构

211

3.4 MySQL基本操作

214

3.5 OSSIM系统迁移

215

3.5.1 迁移准备

215

3.5.2 恢复OSSIM

216

3.6 OSSIM数据库常见问题解答

218

3.7 小结

227

第4章 OSSIM关联分析技术

228

4.1 关联分析技术背景

228

4.1.1 当前的挑战

228

4.1.2 基本概念

229

4.1.3 安全事件之间的关系

229

4.2 关联分析基础

230

4.2.1 从海量数据到精准数据

230

4.2.2 网络安全事件的分类

231

4.2.3 Alarm与Ticket的区别

235

4.2.4 使用Ticket

236

4.2.5 加入知识库

237

4.2.6 安全事件提取

238

4.2.7 OSSIM的关联引擎

238

4.2.8 事件的交叉关联

240

4.3 报警聚合

241

4.3.1 报警样本举例

241

4.3.2 事件聚合

242	
4.3.3 事件聚合举例	243
4.3.4 事件聚合在OSSIM中的表现形式	244
4.3.5 SIEM中的冗余报警	245
4.3.6 合并相似事件	245
4.3.7 同类事件的判别	246
4.3.8 合并流程	247
4.3.9 事件映射	247
4.3.10 Ossec 的报警信息的聚类	247
4.3.11 Ossec与Snort 事件合并	249
4.4 风险评估方法	249
4.4.1 风险评估三要素	249
4.4.2 Risk & Priority & Reliability的关系实例	251
4.4.3 动态可信度值 (Reliability)	254
4.4.4 查看SIEM不同事件	254
4.5 OSSIM系统风险度量方法	256
4.5.1 风险判定	256
4.5.2 事件积累过程	258
4.6 OSSIM中的关联分类	260
4.6.1 关联分类	260
4.6.2 关联指令分类	261
4.6.3 指令组成	263
4.6.4 读懂指令规则	265
4.6.5 Directive Info	266
4.7 新建关联指令	267

4.8 OSSIM的关联规则	270
4.8.1 关联指令配置界面	271
4.8.2 构建规则	274
4.9 深入关联规则	276
4.9.1 基本操作	276
4.9.2 理解规则树	277
4.9.3 攻击场景构建	281
4.9.4 报警聚合计算方法	281
4.10 自定义策略实现SSH登录失败告警	282
4.11 小结	285
第5章 OSSIM系统监测工具	286
5.1 Linux性能评估	286
5.1.1 性能评估工具	286
5.1.2 查找消耗资源的进程	288
5.2 OSSIM压力测试	288
5.2.1 软硬件测试环境	288
5.2.2 测试项目	289
5.2.3 测试工具	289
5.2.4 IDS测试工具Nidsbench	292
5.3 性能分析工具实例	294
5.3.1 sar	295
5.3.2 vmstat	295
5.3.3 用iostat分析I/O子系统	296
5.3.4 dstat	297
5.3.5 iotop	

298	
5.3.6 atop	299
5.3.7 替代netstat的工具ss	299
5.4 OSSIM平台中MySQL运行状况	299
5.4.1 影响MySQL性能的因素	299
5.4.2 系统的IOPS	301
5.5 Syslog压力测试工具——Mustsyslog使用	302
5.5.1 安装mustsyslog	302
5.5.2 日志模板设计	304
5.5.3 日志标签说明	305
5.5.4 域标签举例	305
5.6 常见问题解答	305
5.7 小结	321
第6章 Snort规则分析	322
6.1 预处理程序	322
6.1.1 预处理器介绍	322
6.1.2 调整预处理程序	329
6.1.3 网络攻击模式分类	330
6.2 Snort日志分析利器	332
6.3 Snort日志分析	332
6.3.1 工作模式	332
6.3.2 输出插件	337
6.4 Snort 规则编写	343
6.4.1 Snort 规则分析	344
6.4.2 规则组成及含义	345

6.4.3 编写Snort规则	351
6.4.4 手工修改Suricata规则	354
6.4.5 启用新建的ET规则	354
6.4.6 应用新规则	355
6.4.7 主动探测与被动探测	356
6.5 可疑流量检测技术	356
6.5.1 通过特征检测	356
6.5.2 检测可疑的载荷	356
6.5.3 检测具体元素	357
6.5.4 OSSIM中的Snort规则与SPADE检测	358
6.5.5 恶意代码行为特征分析	358
6.5.6 蜜罐检测	359
6.6 Snort规则进阶	360
6.6.1 可疑流量的报警	360
6.6.2 空会话攻击漏洞报警	361
6.6.3 用户权限获取	361
6.6.4 失败的权限提升报警规则	362
6.6.5 企图获取管理员权限	362
6.6.6 成功获取管理员权限	362
6.6.7 拒绝服务	363
6.7 高速网络环境的应用	365
6.7.1 Suricata VS Snort	365
6.7.2 PF_ring工作模式	365
6.8 网络异常行为分析	366
6.8.1 流程分析	

366	
6.8.2 举例	367
6.10 小结	368
第三篇 实战篇	
第7章 OSSIM日志收集与分析	371
7.1 日志分析现状	371
7.1.1 日志记录内容	372
7.1.2 日志中能看出什么	373
7.1.3 日志分析的基本工具及缺陷	373
7.1.4 海量日志收集方式	374
7.2 日志消息格式与存储	374
7.2.1 日志消息格式	374
7.2.2 OSSIM下的日志查询比较	375
7.2.3 日志的导出	376
7.2.4 日志分类可视化	377
7.2.5 基于文本格式的日志	378
7.2.6 基于压缩模式的日志文件	380
7.2.7 日志转储到数据库	380
7.2.8 日志处理及保存时间	381
7.2.9 日志系统保护	381
7.2.10 日志轮询	381
7.2.11 OSSIM分布式系统中日志存储问题	382
7.3 日志协议Syslog	382
7.3.1 常见日志收集方式	383
7.3.2 日志的标准化	384
7.3.3 主流日志格式介绍	

384	
7.3.4	Syslog日志记录级别
386	
7.3.5	Syslog.conf配置文件
386	
7.3.6	用Tcpdump分析Syslog数据包
388	
7.3.7	Syslog的安全漏洞
388	
7.3.8	配置SNMP
388	
7.4	原始日志格式对比
389	
7.5	插件配置步骤
390	
7.6	插件导入
391	
7.7	插件注册操作实例
391	
7.8	Agent插件处理日志举例
395	
7.8.1	收集与处理过程
395	
7.8.2	常见Windows日志转换syslog工具
397	
7.8.3	Windows日志审核
398	
7.8.4	收集Windows平台日志
398	
7.8.5	收集Cisco 路由器日志
399	
7.9	Rsyslog配置
400	
7.9.1	Rsyslog配置详解
400	
7.9.2	Rsyslog配置参数含义
401	
7.9.3	选择合适的日志级别
401	
7.10	网络设备日志分析与举例
402	
7.10.1	路由器日志分析
403	
7.10.2	交换机日志分析
403	
7.10.3	防火墙日志分析
405	
7.10.4	收集CheckPoint设备日志
407	

- 7.10.5 Aruba (无线AP) 的日志
408
- 7.11 Apache日志分析
409
 - 7.11.1 日志作用
409
 - 7.11.2 日志格式分析
410
 - 7.11.3 日志统计举例
410
 - 7.11.4 错误日志分析
411
- 7.12 Nginx日志分析
413
 - 7.12.1 基本格式
413
 - 7.12.2 将Nginx日志发送到Syslog
415
- 7.13 FTP日志分析
415
 - 7.13.1 FTP日志分析
415
 - 7.13.2 分析vsftpd.log和xferlog
416
 - 7.13.3 将Linux的 Vsftp日志发送到OSSIM
418
- 7.14 iptables 日志分析
419
 - 7.14.1 iptables日志分析
419
 - 7.14.2 iptables日志管理范例
421
 - 7.14.3 输出iptables日志到指定文件
422
- 7.15 Squid服务日志分析
425
 - 7.15.1 Squid日志分类
425
 - 7.15.2 典型Squid访问日志分析
425
 - 7.15.3 Squid时间戳转换
426
 - 7.15.4 将Squid的日志收集到OSSIM
427
- 7.16 DHCP 服务器日志
428
- 7.17 收集Windows日志
430
 - 7.17.1 OSSIM日志处理流程

431	
7.17.2	通过Snare转发Windows日志
431	
7.17.3	通过WMI收集Windows日志
435	
7.17.4	配置OSSIM
436	
7.17.5	Snare与WMI的区别
437	
7.18	小结
438	
第8章	OSSIM流量分析与监控
439	
8.1	用NetFlow分析异常流量
439	
8.1.1	流量采集对业务的影响
440	
8.1.2	NetFlow的Cache管理
441	
8.1.3	NetFlow的输出格式
441	
8.1.4	NetFlow的采样机制
441	
8.1.5	NetFlow采样过滤
441	
8.2	NetFlow在监测恶意代码中的优势
443	
8.2.1	NetFlow的性能影响
444	
8.2.2	NetFlow在蠕虫病毒监测的应用
444	
8.2.3	网络扫描和蠕虫检测的问题
445	
8.2.4	NetFlow与谷歌地图的集成显示
448	
8.2.5	其他异常流量检测结果分析
449	
8.3	OSSIM下NetFlow实战
450	
8.3.1	组成
450	
8.3.2	关键参数解释
452	
8.3.3	Sensor中启用NetFlow
453	
8.3.4	Nfsen数据流的存储位置
454	
8.3.5	NetFlows抽样数据保存时间
456	

8.3.6 NetFlow的读取方式	456
8.3.7 nfdump的作用	458
8.3.8 将NetFlow数据集成到Web UI的仪表盘	458
8.3.9 分布式环境下NetFlow数据流处理	459
8.4 OSSIM流量监控工具综合应用	463
8.4.1 Ntop流量采集方式	463
8.4.2 Ntop监控	464
8.4.3 数据大小分析	469
8.4.4 流量分析	470
8.4.5 协议分析	474
8.4.6 负载分析	475
8.4.7 Ntop应用于网络视频监控	476
8.4.8 Ntop 的风险旗帜标示	478
8.4.9 升级到Ntopng	481
8.5 故障排除	482
8.5.1 多网卡问题	482
8.5.2 Ntop Web页面打开缓慢对策	483
8.5.3 “ Sensor not available ” 故障对策	483
8.5.4 暂停Ntop服务	484
8.5.5 管理员密码遗忘对策	484
8.6 用Nagios监视	485
8.6.1 Nagios实现原理	486
8.6.2 利用NRPE 插件实现服务器监控	486
8.6.3 Nagios的Web界面	489
8.6.4 Naigos插件	

494	
8.6.5 Nagios扩展NRPE	
499	
8.6.6 监控开销	
500	
8.6.7 OSSIM系统中应用Nagios监控资源	
500	
8.6.8 Nagios报错处理	
502	
8.6.9 被动资产检测PRADS	
503	
8.6.10 性能监控利器Munin	
504	
8.7 Nagios配置文件	
505	
8.7.1 主机定义	
506	
8.7.2 服务定义	
507	
8.8 第三方监控工具集成	
507	
8.8.1 OSSIM 2.3的集成	
508	
8.8.2 OSSIM 4.1的集成	
509	
8.8.3 OSSIM 4.6的集成	
510	
8.8.4 Sensor安装Cacti	
511	
8.8.5 安装Zabbix	
513	
8.9 硬件监控	
514	
8.9.1 IPMI	
514	
8.9.2 lm-sensors	
516	
8.9.3 hddtemp	
516	
8.10 小结	
517	
第9章 OSSIM应用实战	
518	
9.1使用OSSIM系统	
518	
9.1.1 初识OSSIM Web UI	
518	
9.1.2 OSSIM 4.8界面	
521	

9.1.3 OSSIM控制中心：AlienVault Center	523
9.1.4 基于角色的访问权限控制	524
9.1.5 仪表盘详解	527
9.2 OSSIM的Web UI菜单结构	529
9.3 OSSEC架构与配置	531
9.3.1 OSSEC架构	531
9.3.2 OSSEC Agent端进程	531
9.3.3 OSSEC Server端	534
9.3.4 OSSEC配置文件和规则库	535
9.3.5 测试规则	537
9.3.6 分布式系统中OSSEC Agent的管理	537
9.3.7 OSSEC日志存储	538
9.3.8 OSSEC Agent安装	539
9.3.9 OSSEC触发的关联分析报警	550
9.3.10 其他HIDS应用	552
9.4 资产Assets管理	553
9.4.1 资产发现	554
9.4.2 资产地图定位	555
9.4.3 扫描控制参数	555
9.4.4 资产列表	556
9.4.5 资产管理工具	558
9.4.6 资产分组	560
9.4.7 资产快速查找	561
9.4.8 设置Nmap扫描频率	562
9.4.9 OCS检测频率	

562	
9.5	OpenVAS扫描模块分析
562	
9.5.1	扫描流程控制
563	
9.5.2	扫描插件分析
564	
9.5.3	脚本加载过程
568	
9.5.4	NASL脚本介绍
569	
9.6	OpenVAS脚本分析
569	
9.6.1	OpenVAS脚本类别
570	
9.6.2	同步OpenVAS插件
570	
9.7	漏洞扫描实践
575	
9.7.1	漏洞库
575	
9.7.2	常见漏洞发布网站
577	
9.7.3	手动更新CVE库
578	
9.7.4	采用OpenVAS扫描
578	
9.7.5	扫描过程
582	
9.7.6	变更扫描策略
584	
9.7.7	Nmap与OpenVAS的区别
587	
9.7.8	分布式漏洞扫描
588	
9.7.9	设置扫描用户凭证
589	
9.7.10	扫描频率
590	
9.7.11	漏洞扫描超时问题
590	
9.8	OpenVAS扫描故障排除
591	
9.8.1	常见OpenVAS故障三则
591	
9.8.2	OpenVAS故障分析
594	
9.9	配置OSSIM报警
598	

9.9.1 基本操作	598
9.9.2 实例	599
9.10 OSSIM在蠕虫预防中的应用	602
9.10.1 多维度分析功能	603
9.10.2 发现异常流量	603
9.10.3 蠕虫分析	604
9.10.4 流量分析	605
9.10.5 协议分析	607
9.11 时间线分析方法	608
9.11.1 时间线分析法的优势	608
9.11.2 实例	608
9.12 利用OSSIM进行高级攻击检测	610
9.12.1 误用检测与异常检测	610
9.12.2 绘制Shellcode代码执行流程图	613
9.12.3 收集异常行为流量样本	614
9.13 合规管理及统一报表输出	615
9.13.1 合规管理目标	615
9.13.2 主要技术	615
9.13.3 什么是合规	616
9.13.4 理解PCI合规遵从	616
9.13.5 报表类型	619
9.13.6 日志合规检测	621
9.13.7 报表合规性	624
9.14 小结	627
第10章 基于B/S架构的数据包捕获分析	

628	
10.1	数据包捕获
628	
10.1.1	数据包捕获设定
629	
10.1.2	抓包区域说明
630	
10.1.3	抓包时提示“ This traffic capture is empty ”的解决办法
631	
10.1.4	远程故障排除案例
631	
10.2	数据包过滤种类
632	
10.3	过滤匹配表达式实例
634	
10.3.1	过滤基础
634	
10.3.2	协议过滤
634	
10.3.3	对端口的过滤
635	
10.3.4	对包长度的过滤
635	
10.3.5	ngrep过滤
636	
10.4	命令行工具tshark和dumpcap
637	
10.4.1	tshark应用基础
637	
10.4.2	dumpcap使用
638	
10.4.3	用tshark分析pcap
638	
10.5	使用tcpdump过滤器
641	
10.5.1	tcpdump过滤器基础
641	
10.5.2	其他常见过滤器使用方法
642	
10.5.3	通过Traffic Capture抓包存储
643	
10.6	针对IE浏览器漏洞的攻击分析
644	
10.7	小结
648	
	参考文献
649	

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。

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。

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:www.tushu111.com