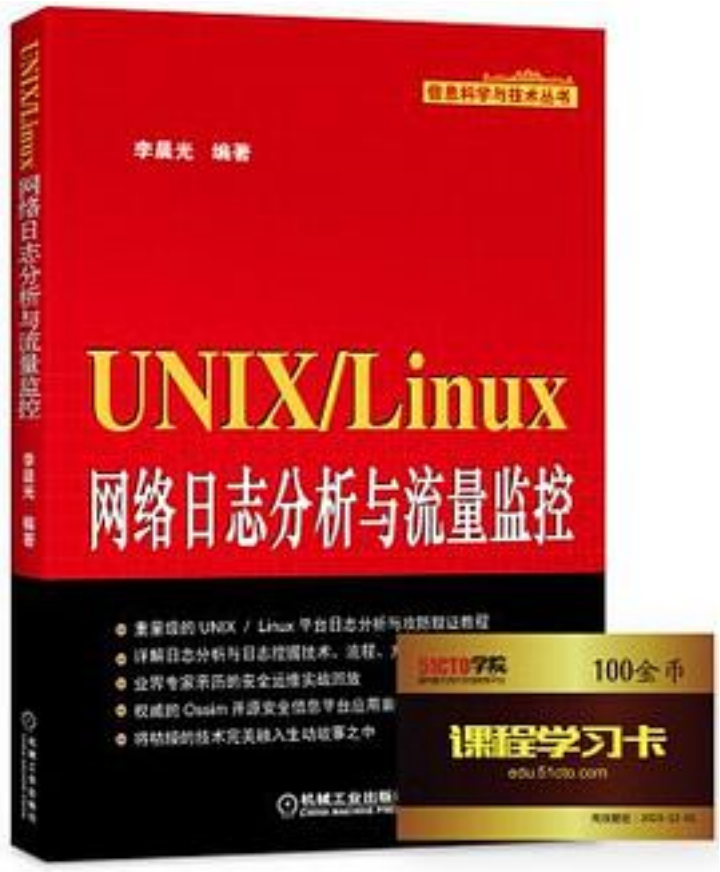
UNIX/Linux网络日志分析与流量监控



UNIX/Linux网络日志分析与流量监控_下载链接1_

著者:李晨光

出版者:机械工业出版社

出版时间:2014-12-1

装帧:平装

isbn:9787111479611

《UNIX/Linux网络日志分析与流量监控》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。

作者介绍:

李晨光，毕业于中国科学院研究生院，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；曾获2011~2013年度全国IT博客10强。从事IDC机房网络设备运维十多年，持有多个IT认证；对Linux/UNIX、网络安全防护有深入研究。曾出版畅销书《Linux企业应用案例精解》和《Linux企业应用案例精解第2版》，多次在国内信息安全大会发表技术演讲，2012年受邀担任中国系统架构师大会（SACC）运维开发专场嘉宾主持人；先后在国内《计算机安全》、《程序员》、《计算机世界》、《网络运维与管理》、《黑客防线》等专业杂志发表论文六十余篇，撰写的技术博文广泛刊登在51CTO、IT168、ChinaUnix、赛迪网、天极网、比特网等国内知名IT网站。

目录: 第一篇 日志分析基础

14.6 风险评估方法
14.7 OSSIM关联分析技术
14.8 OSSIM日志管理平台
14.9 OSSIM系统中的IDS应用
14.10 OSSIM流量监控工具应用
14.11 OSSIM应用资产管理
14.12 OSSIM在蠕虫预防中的应用
14.13 监测shellcode
14.14 OSSIM在漏洞扫描中的应用
14.15 常见OSSIM应用问答
・・・・・・(收起)

UNIX/Linux网络日志分析与流量监控_下载链接1_

标签

日志分析与计算机取证

网络日志分析

Linux

Linux/Unix

安全

日志分析实战

日志分析

防火墙

评论

结构混乱，章节排序就可知，案例发散，应急响应就是按时间节点的事件回溯，讲求清晰明了，书中案例掺杂了太多故事性，画蛇添足，最后一章才是干货，普及、阐述了O

SSIM的系统特性和功能，应该是首本涉及此系统的中文书。

以故事为例，内容很实用

不错，算是这类书里我见到过比较好的了

少见的日志分析图书，里面那些攻防案例，很丰富，利用日志分析和计算机取证技术分析到位，读故事，学技术的思路，不错。

UNIX日志分析全面，案例读起来放不下手。

从论坛看到介绍，在书店原价买的，介绍日志分析内容比较多，一看，挺实在，几十块花的也值了。

那些取证的案例非常难得，结合日志分析来讲解，收获挺大的。

对Linux系统的各种服务日志分析深入，对于日志攻击的案例颇为生动，详细，有点像看电视剧的感觉，例举的各种攻击方法案例很有代表性，对安全工作者可以起到警示教育作用，很赞哦！

看了日志分析案例的前4章，感觉不错，充实，有不小的收获，继续... ...

偏网络安全方向的各种日志分析，案例涉及比较全面，值得一读。

日志分析这本书介绍的比较全面，案例生动而有趣。

这个日志分析主题很不多见，大致看了内容，不错，再细细品味。

从学校毕业都工作这几年，也看过不少Linux图书，其中不乏国外和国内的一些经典教材，在书店看到这本书名，让我眼前一亮，翻看目录，是我有了阅读兴趣，看了里面的案例，让我迅速决定入手，真不错啊。

从Unix/Linux系统运维角度和计算机安全取证的角度阐述日志分析，在深入到日志的收集与管理上，每章都有几个出色的案例，非常有启发，感觉读取来不累。

偏网络安全的日志分析，立意比较新颖，介绍的日志分析内容贴近实战。

最近做日志收集分析的项目正好用上，很不错!

有关日志的内容实用，全面，具有代表性的案例分析到位。

这本日志分析教程确实挺基础的，案例丰富，也比较全面。

正在读，日志分析本就不容易，看得出作者还是有两把刷子。

分析日志的种类比较基础，相对全面，案例分析的中的攻击类型有比较典型。

书评

日志分析本身而言挺复杂，而且枯燥。
但作者能将一些典型的案例汇总到一起，写出来还是真不错，当作床头书来读。前两章的日志基础适合入门来阅读，看来计算机网络，取证分析是基本功。里面的学习卡也能派上点用场啦，呵呵。

喜欢的读这种内容丰富的书，必须动脑子才能读懂，越读越有兴趣。对于Apache,Ftp,DHCP,DNS,IPtables各种服务,防火墙的日志都将到了。
每天睡觉前会看上1-2个案例，分析过程到位，解决方法能给我以启迪，非常不错，还能提供工具下载，考虑的很是周到呀。

对Linux系统的各种服务（Apache,FTP,DHCP,SAMBA,DNS等等）日志分析深入，对于日志攻击的案例颇为生动，详细，有点像看电视剧的感觉，例举的各种攻击方法案例很有代表性，对安全工作者可以起到警示教育作用，很赞！

喜欢书中介绍的OSSIM技术，各种日志涉及面也比较拳全面，把零散分布的日志集中讲解分析，对于日志分析理解很有帮助。
书中的案例防护对我维护系统安全也有帮助。尤其是网络流量收集监控技术，特别适用于目前我管理的网路检测需求，对于OSSIM的安装使用，尤其是在异常流量监测...

这种日志分析我喜欢。
Linux下各种服务的日志分析挺到位的，告诉你怎么识别日志怎么查找路径，最让人难忘的是那些攻防案例和计算机取证案例，读起来挺有意思的。
最让人感到贴心的是，连书中的实验环境和软件都系统集中下载，赞一个。

日志分析的内容很真实。
这本书是从运维的工作实际出发来写，看得出是从实战中长期沉淀的经验，分享的攻防案例很难得，吸取了不少好的经验。
这本书是LInux运维和网络运维SIEM、SOC从业人员必读书籍。

有日志分析基础，看案例更有意思，没有专业书籍那么古板，读那些日志分析数据包抓包分析的案例时，有点像看现实版的黑客帝国，逻辑性强思路清晰，像渗透攻击、SQL注入、跳板攻击很多都只能了解一些理论基础的内容，但这本书里中却用一些个真实的故事表现出来，我感觉印象挺深刻...

讲解细致，日志分析全面。
作者将自己的经历融入案例，介绍的都是些干货，虽然有些命令不太明白，但读整体案例的过程，就仿佛福尔摩斯在向华生讲述整个案情的来龙去脉，逐步掌握分析Unix日志的窍门。 不错，这本书还是值得收藏的。
