

《UNIX/Linux网络日志分析与流》

图书基本信息

书名：《UNIX/Linux网络日志分析与流量监控》

13位ISBN编号：9787111479610

出版时间：2014-12-1

作者：李晨光

页数：448

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

《UNIX/Linux网络日志分析与流》

内容概要

《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。

《UNIX/Linux网络日志分析与流》

作者简介

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。

书籍目录

第一篇 日志分析基础

第1章 网络日志获取与分析

- 1.1 网络环境日志分类
- 1.2 Web日志分析
- 1.3 FTP服务器日志解析
- 1.4 用LogParser分析Windows系统日志
- 1.5 Squid服务日志分析
- 1.6 NFS服务日志分析
- 1.7 iptables日志分析
- 1.8 Samba日志审计
- 1.9 DNS日志分析
- 1.10 DHCP服务器日志
- 1.11 邮件服务器日志
- 1.12 Linux下双机系统日志
- 1.13 其他UNIX系统日志分析GUI工具
- 1.14 可视化日志分析工具

第2章 UNIX/Linux系统取证

- 2.1 常见IP追踪方法
- 2.2 重要信息收集
- 2.3 常用搜索工具
- 2.4 集成取证工具箱介绍
- 2.5 案例一：闪现Segmentation Fault为哪般
- 2.6 案例二：谁动了我的胶片

第3章 建立日志分析系统

- 3.1 日志采集基础
- 3.2 时间同步
- 3.3 网络设备日志分析与举例
- 3.4 选择日志管理系统的十大问题
- 3.5 利用日志管理工具更轻松
- 3.6 用Sawmill搭建日志平台
- 3.7 使用Splunk分析日志

第二篇 日志分析实战

第4章 DNS系统故障分析

- 4.1 案例三：邂逅DNS故障
- 4.2 DNS漏洞扫描方法
- 4.3 DNS Flood Detector让DNS更安全

第5章 DoS防御分析

- 5.1 案例四：网站遭遇DoS攻击
- 5.2 案例五：“太囧”防火墙

第6章 UNIX后门与溢出案例分析

- 6.1 如何防范rootkit攻击
- 6.2 防范rootkit的工具
- 6.3 安装LIDS
- 6.4 安装与配置AIDE
- 6.5 案例六：围堵Solaris后门
- 6.6 案例七：遭遇溢出攻击
- 6.7 案例八：真假root账号

- 6.8 案例九：为rootkit把脉
- 第7章 UNIX系统防范案例
 - 7.1 案例十：当网页遭遇篡改之后
 - 7.2 案例十一：UNIX下捉虫记
 - 7.3 案例十二：泄露的裁员名单
- 第8章 SQL注入防护案例分析
 - 8.1 案例十三：后台数据库遭遇SQL注入
 - 8.2 案例十四：大意的程序员之SQL注入
 - 8.3 利用OSSIM监测SQL注入
 - 8.4 LAMP网站的SQL注入预防
 - 8.5 通过日志检测预防SQL注入
- 第9章 远程连接安全案例
 - 9.1 案例十五：修补SSH服务器漏洞
 - 9.2 案例十六：无辜的“跳板”
- 第10章 Snort系统部署及应用案例
 - 10.1 Snort安装与使用
 - 10.2 Snort日志分析
 - 10.3 Snort规则详解
 - 10.4 基于OSSIM平台的WIDS系统
 - 10.5 案例研究十七：IDS系统遭遇IP碎片攻击
 - 10.6 案例十八：智取不速之客
- 第11章 WLAN案例分析
 - 11.1 WLAN安全漏洞与威胁
 - 11.2 案例十九：无线网遭受的攻击
 - 11.3 案例二十：无线会场的“不速之客”
- 第12章 数据加密与解密案例
 - 12.1 GPG概述
 - 12.2 案例二十一：“神秘”的加密指纹
- 第三篇 网络流量与日志监控
- 第13章 网络流量监控
 - 13.1 网络监听关键技术
 - 13.2 用NetFlow分析网络异常流量
 - 13.3 VMware ESXi服务器监控
 - 13.4 应用层数据包解码
 - 13.5 网络嗅探器的检测及预防
- 第14章 OSSIM综合应用
 - 14.1 OSSIM的产生
 - 14.2 OSSIM架构与原理
 - 14.3 部署OSSIM
 - 14.4 OSSIM安装后续工作
 - 14.5 使用OSSIM系统
 - 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

精彩短评

- 1、案例不错，比价有代表的网络安全事件。
- 2、有关日志的内容实用，全面，具有代表性的案例分析到位。
- 3、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。
- 4、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。
- 5、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！
- 6、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。
- 7、最近做日志收集分析的项目正好用上，很不错!
- 8、以故事为例，内容很实用
- 9、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。
- 10、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OSSIM的系统特性和功能，应该是首本涉及此系统的中文书。
- 11、这本日志分析教程确实挺基础的，案例丰富，也比较全面。
- 12、正在读，日志分析本就不容易，看得出作者还是有两把刷子。
- 13、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。
- 14、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。
- 15、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... ..
- 16、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。
- 17、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。
- 18、UNIX日志分析全面，案例读起来放不下手。
- 19、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。
- 20、公司最近在做一个日志分析可视化的项目，起初日志台凌乱，无从下手，后来公司同事买了这本书，借过来翻了一下，走马关灯的翻了一遍，感觉挺适合我，后来又到店去比较了一起其他日志分析图书，感觉还是满不错的，适合运维人员对服务器日志的理解，涉及到的Apache,DHCP,DNS日志，还有一些鲜为人知的取证工具的使用案例，尤其是OSSIM实战很真实，有内涵。
- 21、日志分析这本书介绍的比较全面，案例生动而有趣。

精彩书评

1、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。

2、这本是年初买的，等我读完的时候，都进入三伏天了。之前工作忙，间断的在读，期间还翻越了老外写的一本日志分析的书，感觉翻译的不好，内容理论居多后来就没看了。现在这两个月又回头仔细品味这本人写的日志分析，还是感觉满好，首先这本书日志分析的面涉及面很广。作者先花了整一章的内容论述自己对各种网络服务产生日志的内容，格式，位置，的基本情况作了详细说明，然后对计算机网络取证又作了实例讲解，中间大量篇幅通过网络攻防的案例来讲述如何分析日志，分析脚本，像这位作者这样能涉及如此全面的日志分析，还比较少见，看来是为安全从业经历丰富的高手所写，尤其是在最后一章介绍的OSSIM监控也首次见到，挺不错，作者的亲生经历也为我工作提供了借鉴。读这本书的时候，基本每一章节我都做了笔记，因为书里涉及很多开源工具，包括一些很新奇的用法，内容较多，保存在了我的笔记中，就不在这里啰嗦了。

3、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。

4、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，我感觉印象挺深刻的，比教科书里介绍的内容，好懂。

5、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。

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