

信息科学与技术丛书

李晨光 编著

UNIX/Linux

网络日志分析与流量监控

- 重量级的 UNIX/Linux 平台日志分析与攻防取证教程
- 详解日志分析与日志挖掘技术、方法、流程
- 业界专家亲历的安全运维实战回放
- 权威的 OSSIM 开源安全信息平台应用案例
- 将枯燥的技术完美融入生动故事中



机械工业出版社
CHINA MACHINE PRESS



信息科学与技术丛书

UNIX/Linux 网络日志 分析与流量监控

李晨光 编著

机械工业出版社

本书以开源软件为基础,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。

图书在版编目(CIP)数据

UNIX/Linux 网络日志分析与流量监控 / 李晨光编著. —北京:机械工业出版社, 2014.12

(信息科学与技术丛书)

ISBN 978-7-111-47961-1

I. ①U… II. ①李… III. ①UNIX 操作系统②Linux 操作系统
IV. ①TP316.8

中国版本图书馆 CIP 数据核字(2014)第 213054 号

机械工业出版社(北京市百万庄大街 22 号 邮政编码 100037)

策划编辑:车 忱

责任编辑:车 忱 责任校对:张艳霞

责任印制:乔 宇

保定市巾画美凯印刷有限公司印刷

2015 年 1 月第 1 版:第 1 次印刷

184mm×260mm·29.5 印张·730 千字

0001—3000 册

标准书号:ISBN 978-7-111-47961-1

定价:79.00 元



凡购本书,如有缺页、倒页、脱页,由本社发行部调换

电话服务

网络服务

社服务中心:(010) 88361066

教材网:<http://www.cmpedu.com>

销售一部:(010) 68326294

机工官网:<http://www.cmpbook.com>

销售二部:(010) 88379649

机工官博:<http://weibo.com/cmp1952>

读者购书热线:(010) 88379203

封面无防伪标均为盗版

出版说明

随着信息科学与技术的迅速发展，人类每时每刻都会面对层出不穷的新技术和新概念。毫无疑问，在节奏越来越快的工作和生活中，人们需要通过阅读和学习大量信息丰富、具备实践指导意义的图书来获取新知识和新技能，从而不断提高自身素质，紧跟信息化时代发展的步伐。

众所周知，在计算机硬件方面，高性价比的解决方案和新型技术的应用一直备受青睐；在软件技术方面，随着计算机软件的规模和复杂性与日俱增，软件技术不断地受到挑战，人们一直在为寻求更先进的软件技术而奋斗不止。目前，计算机和互联网在社会生活中日益普及，掌握计算机网络技术和理论已成为大众的文化需求。由于信息科学与技术 在 电 工、电 子、通 信、工 业 控 制、智 能 建 筑、工 业 产 品 设 计 与 制 造 等 专 业 领 域 中 已 经 得 到 充 分、广 泛 的 应 用，所 以 这 些 专 业 领 域 中 的 研 究 人 员 和 工 程 技 术 人 员 越 来 越 迫 切 需 要 汲 取 自 身 领 域 信 息 化 所 带 来 的 新 理 念 和 新 方 法。

针对人们了解和掌握新知识、新技能的热切期待，以及由此促成的人们对语言简洁、内容充实、融合实践经验的图书迫切需要的现状，机械工业出版社适时推出了“信息科学与技术丛书”。这套丛书涉及计算机软件、硬件、网络和工程应用等内容，注重理论与实践的结合，内容实用、层次分明、语言流畅，是信息科学与技术领域专业人员不可或缺的参考书。

目前，信息科学与技术的发展可谓一日千里，机械工业出版社欢迎从事信息技术方面工作的科研人员、工程技术人员积极参与我们的工作，为推进我国的信息化建设做出贡献。

机械工业出版社

媒体推荐

日志分析是系统管理员的基本技能。UNIX/Linux 系统提供了强大的日志系统，为管理员查找和发现问题提供了强有力的支持。本书以讲故事的形式，将作者的亲身实战经历融入其中，仿佛福尔摩斯在向华生讲述整个案情的来龙去脉，让读者在跟随作者分析的过程中，了解 UNIX/Linux 日志分析的窍门。本书语言通俗易懂，结合案例情景，易于实践操作。

更重要的是，系统管理员（包括各类 IT 从业者）通过本书，不仅可以学习到 UNIX/Linux 日志的作用，还可以举一反三，站在更高的角度看待 IT 运维和系统安全。只有整体看待这些问题，才能增加系统的稳定性和安全性，将系统管理员从日常事务中解脱出来。

——吴玉征 51CTO 副主编（原《计算机世界》报副主编）

本书作者李晨光先生是 51CTO 专家博主，他的文章深受技术同行关注。作者在 2011～2013 年度中国 IT 博客大赛中被评为“十大杰出 IT 博客”，一个如此优秀的博主写的书肯定值得一看。此书详细介绍了 UNIX/Linux 平台下日志分析方法和计算机取证技巧，并以讲故事的形式，介绍日志分析的全过程，其最大亮点是将 UNIX/Linux 系统中枯燥的技术问题，通过生动案例展现出来，每个案例读完后都能让系统管理员们有所收获。读完这本书你一定不会后悔。

——曹亚莉 51CTO 博客总编、51CTO 学院高级运营经理

李晨光老师是 ChinaUnix 专家博主，在 UNIX/Linux 领域研究多年，对日志分析技术有独到见解。这本《UNIX/Linux 网络日志分析与流量监控》是业界第一本基于 UNIX/Linux 环境，讲解应用系统日志收集、分析方法的专著，是李老师多年沉淀的技术结晶。书中采用大量鲜活的案例，生动地展示了系统漏洞防范、恶意代码分析、DoS 分析、恶意流量过滤等安全防护技术，深入分析了诸多系统管理员的错误维护方法及误区，对安全工作者有很好的参考价值。如果你对网络安全、日志分析感兴趣，我们强烈推荐此书。

——ChinaUnix 技术社区

运维人员都很清楚，非常枯燥又不得不做的事情就是服务器日志文件分析和流量监控。尽管现在有很多相关工具和软件，但真正将它们与自己的实际工作相结合时，往往力不从心。这本《UNIX/Linux 网络日志分析与流量监控》以案例驱动的形式从 UNIX/Linux 系统

的原始日志 (Raw Log) 采集、分析到日志审计与取证环节都进行了详细的介绍和说明, 内容非常丰富, 中间还穿插了很多小故事, 毫不枯燥, 让您在轻松的阅读环境中提升自己的日志分析技能。如果是运维人员或想成为运维人员, 您值得拥有!

—ITPUB 技术社区

随着网络威胁的日益严峻，信息安全问题受到越来越多的用户关注。而针对 UNIX/Linux 系统的安全探讨，李晨光老师的这本《UNIX/Linux 网络日志分析与流量监控》显然是非常不错的选择，本书通过一个个生动的案例将 UNIX/Linux 系统下的安全问题进行了深入浅出的剖析，让你可以更好地消化其中的方法和技术，非常值得一读。

—董建伟 IT168 安全频道主编

前言

本书从 UNIX/Linux 系统的原始日志 (Raw Log) 采集与分析讲起, 逐步深入到日志审计与计算机取证环节。书中提供了多个案例, 每个案例都以一种生动的记事手法讲述了网络遭到入侵之后, 管理人员开展系统取证和恢复的过程, 案例分析手法带有故事情节, 使读者身临其境地检验自己的应急响应和计算机取证能力。

本书使用的案例都是作者从系统维护和取证工作中总结、筛选出来的, 这些内容对提高网络维护水平和事件分析能力有重要的参考价值。如果你关注网络安全, 那么书中的案例一定会引起你的共鸣。本书适合有一定经验的 UNIX/Linux 系统管理员和信息安全人士参考。

1. 为什么写这本书

国内已出版了不少网络攻防等安全方面的书籍, 其中多数是以 Windows 平台为基础。但互联网应用服务器大多架构在 UNIX/Linux 系统之上, 读者迫切需要了解有关这些系统的安全案例。所以我决心写一本基于 UNIX/Linux 的书, 从一个白帽的视角, 为大家讲述企业网中 UNIX/Linux 系统在面临各种网络威胁时, 如何通过日志信息查找问题的蛛丝马迹, 修复网络漏洞, 构建安全的网络环境。

2. 本书特点与结构

书中案例覆盖了如今网络应用中典型的攻击类型, 例如 DDoS、恶意代码、缓冲区溢出、Web 应用攻击、IP 碎片攻击、中间人攻击、无线网攻击及 SQL 注入攻击等内容。每段故事首先描述一起安全事件。然后由管理员进行现场勘查, 收集各种信息 (包括日志文件、拓扑图和设备配置文件), 再对各种安全事件报警信息进行交叉关联分析, 并引导读者自己分析入侵原因, 将读者带入案例中。最后作者给出入侵过程的来龙去脉, 在每个案例结尾提出针对这类攻击的防范手段和补救措施, 重点在于告诉读者如何进行系统和网络取证, 查找并修复各种漏洞, 从而进行有效防御。

全书共有 14 章, 可分为三篇。

第一篇日志分析基础 (第 1~3 章), 是全书的基础, 对于 IT 运维人员尤为重要, 系统地总结了 UNIX/Linux 系统及各种网络应用日志的特征、分布位置以及各字段的作用, 包括 Apache 日志、FTP 日志、Squid 日志、NFS 日志、Samba 日志、iptables 日志、DNS 日志、DHCP 日志、邮件系统日志以及各种网络设备日志, 还首次提出了可视化日志分析的实现技术, 首次曝光了计算机系统在司法取证当中所使用的思路、方法、技术和工具, 这为读者有效记录日志、分析日志提供了扎实的基础, 解决了读者在日志分析时遇到的“查什么”、“怎么查”的难题。最后讲解了日志采集的实现原理和技术方法, 包括开源和商业的日志分析系统的搭建过程。

第二篇日志分析实战 (第 4~12 章), 讲述了根据作者亲身经历改编的一些小故事, 再现了作者当年遇到的各种网络入侵事件的发生、发展和处理方法、预防措施等内容, 用一个

个网络运维路上遇到的“血淋淋”的教训来告诫大家，如果不升级补丁会怎么样，如果不进行系统安全加固又会遇到什么后果。这些案例包括 Web 网站崩溃、DNS 故障、遭遇 DoS 攻击、Solaris 安插后门、遭遇溢出攻击、rootkit 攻击、蠕虫攻击、数据库被 SQL 注入、服务器沦为跳板、IP 碎片攻击等。

第三篇网络流量与日志监控（第 13、14 章），用大量实例讲解流量监控原理与方法，例如开源软件 Xplico 的应用技巧，NetFlow 在异常流量中的应用。还介绍了用开源的 OSSIM 安全系统建立网络日志流量监控网络。

本书从网络安全人员的视角展现了网络入侵发生时，当你面临千头万绪的线索时如何从挖掘关键问题，并最终得以解决。书中案例采用独创的情景式描述，通过一个个鲜活的 IT 场景，反映了 IT 从业者在工作中遇到的种种难题。案例中通过互动提问和开放式的回答，使读者不知不觉中掌握一些重要的网络安全知识和实用的技术方案。

本书案例中的 IP 地址、域名信息均为虚构，而解决措施涉及的下载网站以及各种信息查询网站是真实的，具有较高参考价值。书中有大量系统日志，这些日志是网络故障取证处理时的重要证据，由于涉及保密问题，所有日志均做过技术处理。

由于时间紧，能力有限，书中不当之处在所难免，还请各位读者到我的博客多多指正。

3. 本书实验环境

本书选取的 UNIX 平台为 Solaris 和 FreeBSD，Linux 平台主要为 Red Hat 和 Debian Linux。涉及取证调查工具盘是 Deft 8.2 和 Back Track5。在 <http://chenguang.blog.51cto.com>（作者的博客）提供了 DEFT-vmware、BT5-vmware、OSSIM-vmware 虚拟机，可供读者下载学习研究。

4. 致谢

首先感谢我的父母多年来的养育之恩和关心呵护。感谢我在各个求学阶段的老师。尤其要感谢我的妻子，有了她精心的照顾，我才能全身心地投入到创作当中，没有她的支持和鼓励，我无法持之以恒地完成本书。最后要感谢机械工业出版社的车忱编辑，为了提升本书的质量，他花费了大量心血。

李晨光

2014 年 7 月

目 录

出版说明

媒体推荐

前言

第一篇 日志分析基础

第 1 章 网络日志获取与分析	1
1.1 网络环境日志分类	1
1.1.1 UNIX/Linux 系统日志	1
1.1.2 Windows 日志	2
1.1.3 Windows 系统日志	3
1.1.4 网络设备日志	4
1.1.5 应用系统的日志	4
1.2 Web 日志分析	4
1.2.1 访问日志记录过程	5
1.2.2 Apache 访问日志的作用	5
1.2.3 访问日志的位置	5
1.2.4 访问日志格式分析	6
1.2.5 HTTP 返回状态代码	6
1.2.6 记录 Apache 虚拟机日志	7
1.2.7 Web 日志统计举例	7
1.2.8 Apache 错误日志分析	9
1.2.9 日志轮询	11
1.2.10 清空日志的技巧	12
1.2.11 其他 Linux 平台 Apache 日志位置	13
1.2.12 Nginx 日志	13
1.2.13 Tomcat 日志	13
1.2.14 常用 Apache 日志分析工具	14
1.3 FTP 服务器日志解析	15
1.3.1 分析 vsftpd.log 和 xferlog	16
1.3.2 中文对 Vsftp 日志的影响	18
1.3.3 用 Logparser 分析 FTP 日志	18
1.4 用 LogParser 分析 Windows 系统日志	21
1.4.1 LogParser 概述	21
1.4.2 LogParser 结构	21

1.4.3	安装 LogParser	21
1.4.4	LogParser 应用举例	21
1.4.5	图形化分析输出	25
1.5	Squid 服务日志分析	26
1.5.1	Squid 日志分类	26
1.5.2	典型 Squid 访问日志分析	26
1.5.3	Squid 时间戳转换	28
1.5.4	Squid 日志位置	29
1.5.5	图形化日志分析工具	29
1.5.6	其他 UNIX/Linux 平台的 Squid 位置	29
1.6	NFS 服务日志分析	30
1.6.1	Linux 的 NFS 日志	31
1.6.2	Solaris 的 NFS 服务器日志	31
1.7	iptables 日志分析	35
1.8	Samba 日志审计	38
1.8.1	Samba 默认提供的日志	38
1.8.2	Samba 审计	39
1.9	DNS 日志分析	40
1.9.1	DNS 日志的位置	40
1.9.2	DNS 日志的级别	41
1.9.3	DNS 查询请求日志实例解释	41
1.9.4	DNS 分析工具 dnstop	42
1.10	DHCP 服务器日志	43
1.11	邮件服务器日志	45
1.11.1	Sendmail	45
1.11.2	Postfix	45
1.12	Linux 下双机系统日志	46
1.12.1	Heartbeat 的日志	46
1.12.2	备用节点上的日志信息	47
1.12.3	日志分割	47
1.13	其他 UNIX 系统日志分析 GUI 工具	47
1.13.1	用 SMC 分析系统日志	47
1.13.2	Mac OS X 的 GUI 日志查询工具	48
1.14	可视化日志分析工具	49
1.14.1	彩色日志工具 ccze	49
1.14.2	动态日志查看工具 logstalgia	50
1.14.3	三维日志显示工具 gource	51
1.14.4	用 AWStats 监控网站流量	52

第2章 UNIX/Linux 系统取证	57
2.1 常见 IP 追踪方法	57
2.1.1 IP 追踪工具和技术	57
2.1.2 DoS/DDoS 攻击源追踪思路	59
2.2 重要信息收集	60
2.2.1 收集正在运行的进程	60
2.2.2 查看系统调用	61
2.2.3 收集/proc 系统中的信息	64
2.2.4 UNIX 文件存储与删除	64
2.2.5 硬盘证据的收集方法	65
2.2.6 从映像的文件系统上收集证据	66
2.2.7 用 ddrescue 恢复数据	69
2.2.8 查看详细信息	70
2.2.9 收集隐藏目录和文件	71
2.2.10 检查可执行文件	72
2.3 常用搜索工具	72
2.3.1 特殊文件处理	72
2.3.2 The Coroner's Toolkit (TCT 工具箱)	73
2.3.3 Forensix 工具集	74
2.4 集成取证工具箱介绍	74
2.4.1 用光盘系统取证	74
2.4.2 屏幕录制取证方法	75
2.5 案例一：闪现 Segmentation Fault 为哪般	76
这是一起电商网站首页篡改案，管理员小王对各方调查取证，几经周折，对系统 进程、TCP 连接和 Apache 的访问日志进行分析，最终找到了原因。当您看完事件描 述后，您知道小王在 Apache 日志中到底发现了哪些蛛丝马迹？您知道 Apache 出现的 段错误表示什么含义？小王今后该如何防止这种事件再次发生呢？	
事件背景	76
互动问答	80
疑难解析	80
预防措施	82
2.6 案例二：谁动了我的胶片	83
本案描述了 IT 经理张坤在一起广告公司文件泄露的案件中，通过对交换机、服务 器日志和邮件信头进行分析，利用多方面日志内容验证了他的推测，最后他将这些信 息汇总起来，勾勒出了这次攻击事件的全过程。读者在看完事件的描述后，是否知道在 FTP 和 SSH 日志中找到了什么线索？是否知道如何通过攻击者发出的邮件信头找到他 的 IP 地址呢？	
事件背景	83
了解业务流程	83

公司内鬼所为?	84
取证分析	85
遗忘的 Squid 服务器	86
互动问答	88
疑点分析	88
诱捕入侵者	89
疑难解析	90
预防措施	92
第 3 章 建立日志分析系统	93
3.1 日志采集基础	93
3.1.1 Syslog 协议	93
3.1.2 Syslog 日志记录的事件	96
3.1.3 Syslog.conf 配置文件详解	96
3.1.4 Syslog 操作	97
3.1.5 Syslog 的安全漏洞	98
3.1.6 Rsyslog	98
3.1.7 Syslog-ng	100
3.2 时间同步	100
3.2.1 基本概念	100
3.2.2 识别日志中伪造的时间信息	101
3.2.3 时间同步方法	101
3.3 网络设备日志分析与举例	101
3.3.1 路由器日志分析	102
3.3.2 交换机日志分析	102
3.3.3 防火墙日志分析	103
3.3.4 实战:通过日志发现 ARP 病毒	105
3.3.5 实战:交换机环路故障解决案例	108
3.4 选择日志管理系统的十大问题	109
3.5 利用日志管理工具更轻松	114
3.5.1 日志主机系统的部署	115
3.5.2 日志分析与监控	116
3.5.3 利用 Eventlog Analyzer 分析网络日志	117
3.5.4 分析防火墙日志	120
3.6 用 Sawmill 搭建日志平台	120
3.6.1 系统简介	120
3.6.2 部署注意事项	121
3.6.3 安装举例	121
3.6.4 监测网络入侵	124
3.7 使用 Splunk 分析日志	124

3.7.1 Splunk 简介	124
3.7.2 Splunk 安装	124
3.7.3 设置自动运行	125
3.7.4 系统配置	126
3.7.5 设置日志分析目录	127

第二篇 日志分析实战

第4章 DNS 系统故障分析	134
----------------	-----

4.1 案例三：邂逅 DNS 故障	134
-------------------	-----

网管小宋在一次巡检中发现了 DNS 重启的日志，经过仔细分析局域网内外两层防火墙的访问日志，终于发现公司 DNS 服务器的重大漏洞。根据现有的日志分析，你知道攻击者是如何进入网络内部的吗？小宋是如何还原整个事件真相的呢？今后应如何修补此类漏洞？

事件背景	134
查看防火墙日志	136
外部防火墙	137
内部防火墙（NAT）	138
互动问答	138
取证分析	138
问题解答	141
预防措施	141

4.2 DNS 漏洞扫描方法	143
----------------	-----

4.2.1 DNS 扫描的关键技术	143
4.2.2 检查工具	143

4.3 DNS Flood Detector 让 DNS 更安全	145
----------------------------------	-----

4.3.1 Linux 下 DNS 面临的威胁	145
4.3.2 BIND 漏洞	145
4.3.3 DNS 管理	146
4.3.4 应对 DNS Flood 攻击	146
4.3.5 DNS Flood Detector 保安全	147

第5章 DoS 防御分析	149
--------------	-----

5.1 案例四：网站遭遇 DoS 攻击	149
---------------------	-----

本案例描述了某网站受到拒绝服务攻击后，管理员小杨对比防火墙正常/异常状态下的日志，并配合已有的流量监控系统数据，调查经过伪装的 IP 地址，通过多种手段对 DDoS 攻击进行积极防御的过程。

事件背景	149
交互问答	151
事件推理	151
针对措施	152

081	疑难解答	154
181	案例总结	155
181	DoS 扩展知识	156
181	5.2 案例五：“太囧”防火墙	157
181	管理员小杰在一次巡检中发现了防火墙失效，随着深入调查发现防火墙的可用空间	
181	竟然为零。通过大量路由器和防火墙日志对比，得出结论：这是攻击者对其开展的一次网	
181	络攻击所致。小杰管理的网络到底遭受了什么样的攻击，这种攻击又是如何得逞的呢？	
	事件背景	157
181	路由器部分日志文件	159
181	防火墙日志文件	159
281	互动问答	160
181	调查分析	160
181	答疑解惑	161
181	预防措施	162
	第 6 章 UNIX 后门与溢出案例分析	163
101	6.1 如何防范 rootkit 攻击	163
101	6.1.1 认识 rootkit	163
101	6.1.2 rootkit 的类型	163
	6.2 防范 rootkit 的工具	164
	6.2.1 使用 chkrootkit 工具	164
101	6.2.2 Rootkit Hunter 工具	166
101	6.3 安装 LIDS	167
101	6.3.1 LIDS 的主要功能	167
101	6.3.2 配置 LIDS	167
101	6.3.3 使用 Lidsadm 工具	169
101	6.3.4 使用 LIDS 保护系统	170
101	6.4 安装与配置 AIDE	171
101	6.4.1 在 Solaris 中安装 AIDE	172
101	6.4.2 用 AIDE 加固 OSSIM 平台	173
101	6.4.3 Tripwire	175
	6.5 案例六：围堵 Solaris 后门	176
101	管理员张利发现 UNIX 系统中同时出现了多个 inetd 进程，这引起了他的警觉，在	
101	随后的调查取证中又发现了大量登录失败的日志记录，系统中出现了什么异常情况呢？	
101	入侵背景	176
101	分析脚本文件 bd	177
101	分析脚本 doc	179
101	分析脚本文件 ps	180
101	分析脚本 update（一个嗅探器）	180
101	分析脚本 milk	180

发现 need.tar 被植入系统	180
问题	182
答疑解惑	182
预防措施	182
6.6 案例七：遭遇溢出攻击	183
本案例讲述了一起攻击者利用 UNIX 的 RPC 漏洞进行攻击的事件，管理员通过对系统日志和 DNS 日志的深度对比、分析，逐步锁定了攻击者的位置。为什么管理员排除了 CGI 攻击的可能性？他又是如何通过 ls 命令的输出发现系统被做了手脚？	
事件背景	184
分析日志	184
网络入侵检测系统日志（取样）	185
发现系统账号问题	186
问题	189
案例解码	189
分析解答	190
预防措施	191
6.7 案例八：真假 root 账号	191
新老管理员在交接 UNIX 服务器时，新任管理员发现了系统的 passwd、shadow 均被修改，随后管理员开始深入调查，更多的问题浮出水面。服务器到底被做过什么“手脚”呢？	
事件背景	192
恢复 root 密码	193
取证分析	194
互动问答	195
问题解答	196
预防措施	197
6.8 案例九：为 rootkit 把脉	197
管理员小林在一次系统巡检中发现了系统中的 xinetd.conf 文件出现了一个奇怪的记录，这引起了他的高度重视。可是在系统日志中并无异常，唯独 /var/log/secure 日志没有记录任何内容，而且伴随着 Nmap 输出了一些奇怪的端口，服务器 CPU 利用率居高不下。你知道小林的服务器出现了什么问题，又是在何时被攻击的？	
事件背景	197
可疑的/etc/xinetd.conf 记录	198
互动问答	202
事件分析	202
疑难解答	204
预防措施	204
第 7 章 UNIX 系统防范案例	205
7.1 案例十：当网页遭遇篡改之后	205

本案例中讲述了 IIS 服务器网站被篡改的事件，工程师小麦通过 IIS 日志的分析发现了一些线索。攻击者是利用了什么漏洞来攻陷服务器的？对于门户网站（IIS 架构和 LAMP 架构），有哪些防篡改的解决方案呢？	
事件背景	205
日志获取	205
互动问答	206
入侵事件剖析	206
疑难解答	209
防护措施	211
Web 漏洞扫描工具——Nikto	212
7.2 案例十一：UNIX 下捉虫记	214
本案例讲述了一起 UNIX 系统下的蠕虫攻击案例，从一台被攻击的 IIS 服务器日志查起，逐步牵连出系统的错误日志，以及受到蠕虫攻击的 Solaris 系统。种种迹象表明，系统受到了 Unicode 蠕虫攻击。你知道服务器是如何受到攻击的？攻击源在哪里？	
事件背景	214
取证分析	215
互动问答	217
入侵解析	217
Sadmin/IIS 蠕虫分析	217
Unicode 攻击逆向分析	219
问题解答	220
预防措施	221
7.3 案例十二：泄露的裁员名单	221
IT 经理老郭通过在离职同事的计算机中意外发现的日志文件而牵出一起公司高管加密邮件泄露案件，这和交换机的 CAM 表溢出有直接关系。通过分析 Tcpdump 日志，你能否还原事件的始末？	
事件背景	221
取证分析	222
互动问答	223
答疑解惑	224
预防措施	225
第 8 章 SQL 注入防护案例分析	227
8.1 案例十三：后台数据库遭遇 SQL 注入	227
网络管理员收到一封邮件，阅读之后才恍然大悟，原来系统遭到黑客入侵。系统数据库是如何被入侵的呢？为了查清此事，技术人员紧密协作，在分析了大量日志之后找到了系统的漏洞。他们是如何在日志中发现入侵行为的呢？	
案例背景	227
互动问答	230
分析过程	230

疑难解答	231
预防与补救措施	232
8.2 案例十四：大意的程序员之 SQL 注入	232
即使在严格的防火墙策略下，含有漏洞的程序代码也会让入侵者得逞。接下来讲 述了在防护极为严格的网络环境下发生的 SQL 注入案例。	
事件背景	232
互动问答	234
分析取证	234
总结	235
答疑解惑	235
总结	237
预防措施	239
8.3 利用 OSSIM 监测 SQL 注入	239
8.3.1 SQL 注入攻击的正则表达式规则	239
8.3.2 用 OSSIM 检测 SQL 注入	240
8.3.3 OSSIM 系统中的 Snort 规则	241
8.4 LAMP 网站的 SQL 注入预防	242
8.4.1 服务器端的安全配置	242
8.4.2 PHP 代码的安全配置	243
8.4.3 PHP 代码的安全编写	243
8.5 通过日志检测预防 SQL 注入	244
8.5.1 通过 Web 访问日志发现 SQL 攻击	244
8.5.2 用 Visual Log Parser 分析日志	245
第 9 章 远程连接安全案例	247
9.1 案例十五：修补 SSH 服务器漏洞	247
程通过收集的 Web 日志和 SSH 日志发现了 SSH 服务器存在的漏洞，如何配置 SSH 服务才更安全？	
事件背景	247
SSH 被攻击的日志举例	250
加固 SSH 服务器	251
通过 OSSIM 实现 SSH 登录失败告警功能	252
预防措施	254
9.2 案例十六：无辜的“跳板”	255
这一案例讲述某公司的计算机系统被神不知鬼不觉地用来向其他计算机发起大面 积的攻击。管理员通过网络嗅探等取证方法成功捕获了攻击者的实施过程。你如果是该 公司的管理员，将如何防范这种多级跳攻击呢？	
事件背景	255
交互问答	257
案情分析	257