

## <<Snort入侵检测实用解决方案>>

### 图书基本信息

书名：<<Snort入侵检测实用解决方案>>

13位ISBN编号：9787111157014

10位ISBN编号：711115701X

出版时间：2005-1

出版时间：机械工业出版社

作者：科瑞奥

页数：257

译者：吴溥峰,孙默,许诚

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：<http://www.tushu007.com>

## <<Snort入侵检测实用解决方案>>

### 内容概要

本书在介绍入侵检测系统的基础上，对Snort进行深入地剖析，详细介绍了Snort在实际应用中的安装、使用及维护。

全书共14章，分别介绍了入侵检测基础、利用Snort进行入侵检测、剖析Snort、安装Snort的计划、Snort运行的基础——硬件和操作系统、建立服务器、建立传感器、建立分析员控制台、其他操作系统下的安装、调整和减少误报、实时报警、基本规则的编写、升级和维护Snort以及有关入侵防范的高级话题。

本书内容涵盖了Snort实际应用的各个方面。

本书无论是对具体的商业应用，还是对教学、科研工作都有相当大的参考价值。

## <<Snort入侵检测实用解决方案>>

### 作者简介

Jack Koziol是芝加哥地区一家主要财政机构的信息安全长官，负责企业范围内的安全。先前，他在一家在线健康护理公司和网络药店的信息安全部门供职。

Jack为信息安全杂志供稿，并发表了一些有关入侵检测的文章。

他教授有关CISSP考试和“黑客及其防护”的课程。

自从1998年以来，Jack在一些大的生产环境中构建、维护及管理Snort和其他的入侵检测系统。他也为一些专门的应用软件撰写Snort特征集。

## <<Snort入侵检测实用解决方案>>

### 书籍目录

关于作者译者序绪论第1章 入侵检测基础1.1 不同类型的入侵检测系统1.2 检测入侵的方法1.3 攻击的来源1.4 攻击的步骤1.5 入侵检测系统的现状1.6 小结第2章 利用Snort进行网络入侵检测2.1 Snort的规格说明2.2 通过特征检测可疑流量2.3 启发式的可疑流量检测2.4 采集入侵数据2.5 利用输出插件进行报警2.6 分层报警2.7 分布式Snort体系2.8 安全的Snort2.9 Snort的缺陷2.10 小结第3章 剖析Snort3.1 用Libpcap发送Snort包3.2 预处理程序3.3 检测引擎3.4 输出插件3.5 小结第4章 安装Snort的计划4.1 制定入侵检测系统的策略4.2 决定要监控的内容4.3 设计Snort体系结构4.4 维护计划4.5 事件响应4.6 小结第5章 基础——硬件和操作系统5.1 硬件性能的度量5.2 操作系统平台的选择5.3 监控网段5.4 多传感器分流5.5 小结第6章 建立服务器6.1 安装指南6.2 Red hat linux 7.3的安装6.3 后安装任务6.4 安装Snort 服务器组件6.5 小结第7章 建立传感器.....第8章 建立分析员控制台第9章 其他操作系统下的安装方法第10章 调整和减少误报第11章 实时报警第12章 基本规则的编写第13章 升级和维护Snort第14章 入侵防范高级话题附录

<<Snort入侵检测实用解决方案>>

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:<http://www.tushu007.com>