<<Linux网络入侵检测系统>>

图书基本信息

书名：<<Linux网络入侵检测系统>>

13位ISBN编号：9787121004773

10位ISBN编号：7121004771

出版时间：2004-10-1

出版时间：电子工业出版社

作者：刘文涛

页数：277

字数：458000

<<Linux网络入侵检测系统>>

内容概要

本书在介绍入侵检测系统的基本概念和原理的基础上，通过在linux下设计一个典型的基于网络的入侵检测系统来更深入地探讨入侵检测技术。
本书的一大特色是原理概念的讲述和系统的设计相辅相成，紧密联系。
典型系统采用模块化设计思想，分别是网络数据包捕获模块、网络协议分析模块、存储模块、规则解析析模块、入侵检测模块、响应模块和界面管理模块七个模块。
另外，本书还深入讨论了网络数据包捕获技术、协议分析技术、入侵检测技术、入侵事件描述语言的建立、存储技术、多线程技术、界面设计技术等。
本书适合于计算机专业的本科生和研究生阅读，也可供从事计算机工程与应用的科技工作者或网络安全爱好者参考。

<<Linux网络入侵检测系统>>

书籍目录

<<Linux网络入侵检测系统>>

版权说明