

## <<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

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>

## <<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。

## &lt;&lt;Linux网络入侵检测系统&gt;&gt;

## 书籍目录

第1章 网络安全问题及其对策 1.1 网络安全问题 1.2 网络安全目标 1.3 网络面临的主要威胁 1.4 传统网络安全技术 1.5 网络安全模型--PPDR第2章 入侵检测系统概述 2.1 入侵检测的产生及其定义 2.2 入侵检测系统的分类 2.3 入侵检测系统的标准化 2.3.1 入侵检测工作组IDWG 2.3.2 公共入侵检测框架CIDF 2.4 主要入侵检测系统介绍第3章 入侵检测原理 3.1 入侵检测模型 3.1.1 IDES模型 3.1.2 CIDF模型 3.2 入侵检测技术 3.2.1 异常检测 3.2.2 误用检测 3.3 入侵检测的发展方向第4章 Linux网络入侵检测系统设计 4.1 系统设计原理 4.2 主要功能要求 4.3 检测器位置 4.4 数据源 4.5 系统总体结构 4.6 小结第5章 网络数据包捕获模块设计与实现 5.1 Linux内核中TCP/IP协议栈分析 5.2 BPF机制 5.2.1 几种分组捕获机制介绍 5.2.2 BPF过滤机制 5.3 使用libpcap函数库 5.3.1 主要函数介绍 5.3.2 编写步骤 5.3.3 bpf过滤规则 5.4 实现数据包捕获模块第6章 网络协议分析模块设计与实现 6.1 TCP/IP协议分析基础 6.1.1 概述 6.1.2 IP协议 6.1.3 TCP协议 6.1.4 UDP协议 6.1.5 ICMP协议 6.2 协议分析模块的实现过程 6.2.1 协议分析过程 6.2.2 以太网协议分析 6.2.3 ARP协议分析和RARP协议分析 6.2.4 IP协议分析 6.2.5 TCP协议分析 6.2.6 UDP协议分析 6.2.7 ICMP协议分析 6.3 其他协议的分析 6.3.1 DNS协议 6.3.2 DHCP协议 6.3.3 IPX/SPX协议 6.4 使用Libnids库 6.4.1 Libnids库简介 6.4.2 分析TCP连接过程 6.4.3 分析HTTP协议第7章 存储模块设计与实现 7.1 设计原理 7.2 MySQL数据库 7.2.1 安装MySQL数据库 7.2.2 基本操作 7.2.3 基本函数 7.3 存储模块实现 7.3.1 使用PHPMyAdmin管理数据库 7.3.2 设计数据库 7.3.3 实现数据库连接 7.4 数据库分析 7.4.1 分析IP数据包的分布状态 7.4.2 分析总体协议的分布状态 7.4.3 HTTP流量分析第8章 规则解析模块设计与实现 8.1 建立入侵事件描述语言 8.2 特征的选择 8.3 规则格式 8.4 规则选项 8.4.1 IP协议变量 8.4.2 TCP协议变量 8.4.3 UDP协议变量 8.4.4 ICMP协议变量 8.4.5 响应方式 8.5 规则解析模块实现 8.6 小结第9章 入侵事件检测模块设计与实现 9.1 入侵检测方法 9.1.1 模式匹配方法的不足 9.1.2 使用协议分析方法 9.1.3 协议分析技术的优点 9.2 入侵事件检测模块实现 9.2.1 获取协议信息 9.2.2 规则匹配 9.2.3 检测扫描行为 9.3 小结第10章 入侵响应模块设计与实现 10.1 响应的类型 10.2 入侵响应模块实现 10.2.1 采用声音警报的方式来响应 10.2.2 采用灯光闪烁的方式来发警报 10.2.3 使用日志来记录第11章 界面模块设计与实现 11.1 GTK概述 11.2 GTK控件 11.3 使用GTK 11.4 多线程技术 11.4.1 创建线程 11.4.2 结束线程 11.4.3 线程同步 11.4.4 GTKV+多线程 11.5 实现本系统界面模块 11.5.1 本系统界面分布情况 11.5.2 界面模块实现 11.6 小结参考文献及进一步的读物

## <<Linux网络入侵检测系统>>

### 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>