

<<入侵检测技术>>

图书基本信息

书名：<<入侵检测技术>>

13位ISBN编号：9787302082828

10位ISBN编号：7302082820

出版时间：2004-4

出版时间：清华大学出版社

作者：唐正军

页数：226

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>

## <<入侵检测技术>>

### 内容概要

本书全面细致地讲述了入侵检测的各项技术，概念清晰，行文流畅。

全书共分十二章。

第一章和第二章主要介绍了入侵检测相关的历史和概念。

第三章对入侵检测的信息来源，技术分类等做了简要的介绍。

第四章和第五章对基于主机的入侵检测技术和基于网络的入侵检测技术进行了介绍。

第六章介绍了混合型入侵检测技术的特点。

第七章对若干先进入侵检测算法的应用情况做了简要的介绍。

第八章对分布式入侵检测架构的设计问题进行了分析讨论；第九章和第十章分别对入侵检测系统在设计时所要考虑的若干实际问题和入侵检测的响应问题进行了介绍。

第十一章和第十二章对相关的法律问题和未来的技术发展前景做了介绍和展望。

本书适合作为计算机、信息安全、通信等相关专业的高年级本科生和研究生的数学用书，也可供广大网络安全工程技术人员参考。

## <<入侵检测技术>>

### 作者简介

唐正军，现在上海交通大学信息与通信工程流动站从事博士后研究工作。  
近5年来发表学术论文20篇，出版网络安全相关技术著作3部，并参加国家自然科学基金儿863计划等国家重大项目多项。  
同时，申请技术专利和软件版权各1项。

李建华，现任国家863计划信息安全技术专家

## &lt;&lt;入侵检测技术&gt;&gt;

## 书籍目录

第1章 入侵检测技术的历史 1.1 主机审计——入侵检测的起点 1.2 入侵检测基本模型的建立 1.3 技术发展的历程 习题第2章 入侵检测的相关概念 2.1 入侵的定义 2.2 什么是入侵检测 2.3 入侵检测与P2DR模型 习题第3章 入侵检测技术的分类 3.1 入侵检测的信息源 3.2 分类方法 3.3 具体的入侵检测系统 习题第4章 基于主机的入侵检测技术 4.1 审计数据的获取 4.2 用于入侵检测的统计模型 4.3 入侵检测的专家系统 4.4 基于状态转移分析的入侵检测技术 4.5 文件完整性检查 4.6 系统配置分析技术 习题第5章 基于网络的入侵检测技术 5.1 分层协议模型与TCP/IP协议 5.2 网络数据包的截获 5.3 检测引擎的设计 习题第6章 混合型的入侵检测技术 6.1 采用多种信息源 6.2 采用多种检测方法 习题第7章 先进入侵检测技术 7.1 采用先进检测算法的必要性 7.2 神经网络与入侵检测技术 7.3 数据挖掘与入侵检测技术 7.4 数据融合与入侵检测技术 7.5 计算机免疫学与入侵检测技术 7.6 进化计算与入侵检测技术 习题第8章 分布式的入侵检测架构 8.1 应用背景 8.2 需要解决的关键问题 8.3 分布式检测架构的基础设计 8.4 进一步的发展 习题第9章 入侵检测系统的设计考虑 9.1 用户需求分析 9.2 系统安全设计原则 9.3 系统设计的生命周期 习题第10章 入侵检测的响应问题 10.1 响应策略的确定 10.2 选择恰当的响应类型 10.3 响应组件的设计 习题第11章 相关的法律问题 11.1 网络空间中的法律问题 11.2 入侵证据的保全 11.3 处理入侵证据的方法 习题第12章 未来需求与技术发展前景 12.1 技术的发展趋势 12.2 现有入侵检测技术的局限性 12.3 入侵检测的发展前景 习题参考文献

<<入侵检测技术>>

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>