

## <<入侵检测技术导论>>

### 图书基本信息

书名：<<入侵检测技术导论>>

13位ISBN编号：9787111140795

10位ISBN编号：7111140796

出版时间：2004-4

出版时间：机械工业出版社

作者：唐正军

页数：272

字数：434000

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>

## <<入侵检测技术导论>>

### 内容概要

这是一本介绍入侵检测技术的入门书籍。

全书共分为14章，内容包括：黑客攻击主要手段以及入侵检测技术的相关问题；主要操作系统的文件系统和审计机制；基于主机的入侵检测技术知识；RPC技术；早期著名的主机入侵检测系统IDES/NIDES系统；另外一种类型的主机入侵检测技术；网络入侵检测技术的基础设计知识；早期的分布式入侵检测系统AAFID系统。

在本书的第12-14章中，作者阐述了独立工作的成果。

其中包括入侵检测不对称模型的引入、基于神经网络的入侵检测技术以及智能化入侵检测系统的架构设计等。

本书适用于计算机和信息安全专业的高校教师和研究生以及广大网络安全工程技术人员参考之用。

## <<入侵检测技术导论>>

### 书籍目录

出版说明前言第1章 概述 1.1 主要入侵攻击手段简介 1.2 入侵检测与P2DR安全模型 1.3 入侵检测技术分类 1.4 入侵检测系统的CIDF模型 1.5 入侵检测系统的管理、评测问题 1.6 相关的法律问题第2章 UNIX/Linux系统介绍 2.1 UNIX系统简介 2.2 日益流行的Linux操作 2.3 Linux文件系统第3章 审计机制及文件格式 3.1 UNIX操作系统 3.2 Windows 2000操作系统第4章 RPC 4.1 RPC的产生及特点 4.2 RPC的数据表示格式 4.3 RPC协议 4.4 RPC的程序设计 4.5 RPC语言编译器 ( rpcgen ) 第5章 IDES/NIDES系统实例 5.1 引言 5.2 IDES设计模型 5.3 审计数据 5.4 邻域接口 5.5 统计异常检测器 5.6 IDES专家系统 5.7 IDES用户接口 5.8 进一步的发展：NIDES系统第6章 STAT——基于状态转移分析的系统第7章 网络协议族介绍第8章 数据流捕获技术第9章 检测引擎设计第10章 Snort系统分析第11章 AAFID分布式系统第12章 入侵检测的不对称模型第13章 基于神经网络的入侵检测技术第14章 智能化入侵检测系统的设计附录 入侵检测技术FAQ

<<入侵检测技术导论>>

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>