

<<入侵检测>>

图书基本信息

书名：<<入侵检测>>

13位ISBN编号：9787560622637

10位ISBN编号：7560622631

出版时间：2009-8

出版时间：西安电子科技大学出版社

作者：鲜永菊 主编

页数：342

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>>

### 内容概要

作为对防火墙的有益补充，入侵检测系统（IDS）能够帮助网络系统快速发现攻击的发生，它扩展了系统管理员的安全管理能力，提高了信息安全基础结构的完整性。

本书主要内容包括：当前网络安全的主要威胁、攻击行为分析、主动安全防御技术、入侵检测系统基础知识、入侵检测系统中的主要技术、入侵检测的标准、入侵检测系统的架构与设计、入侵检测系统评估、Snort的配置与使用等。

本书可作为高等学校信息安全、信息工程、计算机应用、通信与信息系统、控制工程等相关专业的高年级本科生和硕士研究生的专业教材和参考书籍，也可供需要掌握入侵检测相关知识和从事相关领域开发的人员及其他网络安全领域相关行业人员参考使用。

## &lt;&lt;入侵检测&gt;&gt;

## 书籍目录

第1章 概述 1.1 网络安全的主要威胁 1.1.1 互联网已经进入木马/病毒经济时代 1.1.2 “0Day”等漏洞和系统缺陷令人防不胜防 1.1.3 社会工程学的攻击手段成为病毒入侵的重要途径 1.1.4 网络内部原因所引起的安全威胁 1.2 攻击行为分析 1.3 主动安全防御技术概述 1.3.1 主动安全防御的基本思想 1.3.2 常见主动防御技术 习题1

第2章 入侵检测系统基础知识 2.1 入侵检测系统的基本组成 2.1.1 入侵检测的一般过程 2.1.2 入侵检测系统模型及组件 2.2 入侵检测系统的分类 2.2.1 按IDS数据源的分类方式 2.2.2 按IDS所采用的分析技术分类 2.2.3 其它分类方式 2.3 基于主机的入侵检测系统 2.3.1 基于主机的入侵检测系统的工作原理 2.3.2 基于主机的IDS的优缺点 2.3.3 基于主机的入侵检测系统的分类 2.3.4 基于主机的入侵检测系统的体系结构 2.3.5 基于主机的入侵检测系统的模型分析 2.4 基于网络的入侵检测系统 2.4.1 基于网络的入侵检测系统的工作原理 2.4.2 基于网络的IDS的优缺点 2.4.3 基于网络的入侵检测系统的体系结构 2.4.4 基于网络的入侵检测系统的模型分析 2.5 分布式入侵检测系统 2.5.1 分布式入侵检测系统的设计思想 2.5.2 分布式入侵检测系统的体系结构 2.5.3 分布式入侵检测系统的典型方案分析1 2.5.4 分布式入侵检测系统的典型方案分析2 习题2

第3章 入侵检测系统中的主要技术 3.1 攻击防范技术 3.1.1 网络安全防范的正确策略 3.1.2 密码学基本方法的应用 3.1.3 漏洞探测法 3.1.4 信息流的控制 3.1.5 诱骗法 3.1.6 其它常见攻击防范技术 3.2 入侵检测技术 3.2.1 审计跟踪及分析法 3.2.2 包过滤方法 3.2.3 入侵检测相关的数学模型 3.2.4 入侵检测系统的检测方式 3.2.5 误用检测 3.2.6 异常检测 3.2.7 混合式检测 3.2.8 IPS的高级检测技术 3.2.9 信息的主动收集 3.3 入侵响应技术 3.3.1 响应策略的制定 3.3.2 常见响应方式 3.3.3 主动响应技术 3.4 自动恢复技术 3.4.1 自动恢复技术的相关概念 3.4.2 自动恢复技术实例说明 3.5 入侵取证与反取证技术 3.5.1 计算机入侵取证技术 3.5.2 网络入侵取证技术 3.5.3 反取证技术 3.6 新一代入侵检测产品引入的关键性技术 习题3

第4章 入侵检测标准 4.1 通用入侵检测框架 4.1.1 IDS的体系结构 4.1.2 CIDF的通信机制 4.1.3 CIDF语言 4.1.4 CIDF的API接口 4.2 IDWG的建议草案 4.2.1 入侵检测消息交换格式 4.2.2 入侵检测交换协议 4.2.3 隧道轮廓 4.3 两种标准草案之间的联系 ..... 第5章 入侵检测系统的架构与设计 第6章 入侵检测系统评估 第7章 Snort的配置与使用 附录参考文献

<<入侵检测>>

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>