第一图书网, tushu007.com

<<网络入侵检测原理与技术>>

图书基本信息

书名：<<网络入侵检测原理与技术>>

13位ISBN编号：9787564006341

10位ISBN编号：756400634X

出版时间：2006-1

出版时间：北京理工大学出版社

作者：胡昌振

页数：216

字数：275000

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

第一图书网, tushu007.com

<<网络入侵检测原理与技术>>

内容概要

本书致力于提出一种提高网络入侵检测的检测率、降低误警率的理论和方法，并将其应用于网络入侵检测系统设计中。

本书详细论述了网络入侵检测及其系统设计的原理和技术。

在简要介绍了网络入侵检测的意义、方法、已有技术及存在的问题之后，分别对基于关键主机的异常检测，滥用检测的不确定性知识表达与推理、基于本体的网络协同攻击检测，基于主动知训库系统的滥用检测系统，网络入侵检测机器学习和分布式入侵检测与信息融合等技术、原理与方法进行了详细的论述，最后对网络入侵检测技术的发展与趋势进行了分析。

本书是一本反映网络入侵检测技术最新研究成果的技术专著，内容取材于多篇博士论文的研究成果，可供从事信息安全技术工作的技术人员和研究人员参考，也可作为信息安全技术及相关学科的研究生教材。

第一图书网, tushu007.com

<<网络入侵检测原理与技术>>

书籍目录

第一章 导论 1.1 信息安全概念体系 1.2 信息安全保障体系 1.3 网络入侵检测技术 1.4 网络入侵检测的误警分析 1.5 本书的主要工作与特色 参考文献第二章 基于关键主机的异常检测技术 2.1 基于关键主机的异常检测系统体系结构 2.2 基于系统调用序列的异常检测方法 2.3 基于网络输入流的异常检测方法 2.4 基于粗糙集的告警信息融合方法 参考文献第三章 滥用检测的不确定性知识表达与推理技术 3.1 基于模糊不确定性推理的入侵检测方法 3.2 模糊攻击知识库的建立 3.3 基于模糊Petri网的攻击知识表示与推理 3.4 基于Petri网的攻击知识库校验 3.5 基于模糊神经网络的知识更新与规则提取 参考文献第四章 基于本体的网络击检测技术 4.1 网络安全本体 4.2 协同攻击检测的检测方法 4.3 基于本体的协同攻击检测系统 4.4 入侵检测本体对遗留或异构Agent的重构框架 参考文献第五章 基于主动知识库系统的滥用检测系统 5.1 主动知识库系统 5.2 基于主动专家系统的滥用检测系统 5.3 检测知识的ECA规则表示 5.4 基于ECA规则的入侵检测系统 参考文献第六章 网络入侵检测机器学习方法 ……第七章 分布式入侵检测与信息融合第八章 网络入侵检测技术的发展与趋势

第一图书网, tushu007.com

编辑推荐

《网络入侵检测原理与技术(第2版)》由北京理工大学出版社出版。

第一图书网, tushu007.com

<<网络入侵检测原理与技术>>

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