第一图书网, tushu007.com

<<网络入侵分析与入侵响应>>

图书基本信息

书名：<<网络入侵分析与入侵响应>>

13位ISBN编号：9787564043834

10位ISBN编号：7564043830

出版时间：2011-3

出版时间：北京理工大学出版社

作者：穆成坡

页数：155

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

内容概要

本书主要对入侵检测系统报警的各类分析处理技术、入侵在线风险评估技术和入侵响应决策技术进行介绍。
内容包括：入侵检测系统报警处理所涉及的概念、标准、语言、分类和结构；报警聚合、报警统计、报警验证和报警关联等报警分析处理方法和模型；典型的报警处理工具；报警分级技术；定性和定量的在线入侵风险评估技术；自动入侵响应所涉及的关键技术、响应目的、响应策略、响应因素和响应措施等有关内容；各类入侵响应时机决策和入侵响应措施决策的方法和模型；各类网络安全设备的特点、使用和部署方法等。

本书可作为计算机、信息安全等相关专业高年级本科生、研究生的教学参考书，也可供网络安全领域的科研、设计和管理人员参考。

书籍目录

第1章 引论
1.1 网络安全技术及其发展趋势
1.2 防火墙技术
1.2.1 防火墙及其作用
1.2.2 防火墙的分类
1.2.3 防火墙存在的问题
1.3 入侵检测技术
1.4 入侵响应技术
1.5 漏洞扫描技术
1.6 入侵检测报警分析与自动入侵响应技术的重要性
1.6.1 入侵检测报警分析、处理的重要性
1.6.2 自动入侵响应的重要性
第2章 入侵检测系统的报警分析与处理
2.1 引言
2.1.1 入侵检测系统的报警信息
2.1.2 入侵检测与报警处理
2.2 报警处理相关概念、语言与标准
2.2.1 相关概念
2.2.2 报警处理语言
2.2.3 报警数据格式标准IDMEF
2.3 报警聚合与关联系统的体系结构
2.4 报警的分类与分析
2.5 报警聚合
2.5.1 聚合算法与目标
2.5.2 自适应的报警聚合
2.6 报警统计
2.6.1 报警统计目标
2.6.2 报警确信度学习实例
2.7 报警验证
2.7.1 报警验证目标与算法
2.7.2 基于多层模糊综合评判的报警验证
2.8 报警关联
2.8.1 关联目标与算法
2.8.2 基于模糊综合评判的报警关联
2.9 计算与分析
2.9.1 报警验证计算与分析
2.9.2 报警关联计算与分析
2.10 实验与分析
2.11 报警处理方法的选择
2.12 报警的分析与处理工具
2.12.1 入侵检测信息处理平台ACIDBASE
2.12.2 SnortSnarf
第3章 安全事件分级与在线入侵风险评估
3.1 在线风险评估概述
3.2 安全事件分级

3.3 定性风险评估法
3.4 基于规则的在线风险评估模型
3.5 层次化在线风险评估的概念与思想
3.6 服务层次上的风险评估
3.6.1 服务层次的风险指数计算
3.6.2 风险分布与风险状态确定
3.7 主机层次上的风险评估
3.8 网络层次上的风险评估
3.9 层次化风险评估实例
3.10 总结
第4章 自动入侵响应技术
4.1 引言
4.2 自动入侵响应中的关键技术
4.3 响应目的与策略
4.4 入侵响应决策中的响应因素
4.4.1 响应因素统计
4.4.2 响应因素分类
4.4.3 响应因素的分析与选择
4.5 针对入侵响应决策的攻击分类
4.6 响应措施分类
4.7 响应时机决策
4.8 响应措施决策
4.8.1 静态映射模型
4.8.2 动态映射模型
4.8.3 成本敏感模型
4.8.4 基于响应负面效应最小原则模型
4.8.5 基于实时入侵风险评估的模型
4.9 现有响应决策模型的问题
4.10 小结
第5章 安全设备部署与使用
5.1 现有网络安全状况分析
5.2 防火墙部署与使用
5.3 网闸的部署使用
5.4 入侵检测系统部署使用
5.5 自动入侵响应系统的部署使用
5.6 入侵防御系统部署与使用
5.7 统一威胁管理系统的部署与使用
5.8 其他网络安全措施与设备的部署
5.8.1 VI,AN的划分与使用
5.8.2 访问列表ACL
5.8.3 网络地址转换NAT技术
5.8.4 安全交换机
5.9 小结
参考文献

章节摘录

版权页：插图：第3章 安全事件分级与在线入侵风险评估3-1在线风险评估概述1983年美国国家计算机安全中心颁布第一个信息安全评估标准《可信计算机系统评估准则》（TCSEC）。
由于TCSEC存在不足，欧洲国家在1991年发布了自己制定的《信息技术安全评估准则》（ITSEC）。
TCSEC采用了TCSEC框架，但做了更加实用的改进。
目前，国际上公认的信息安全评估标准《信息技术安全评估通用准则》，即CC准则，已经被接纳为.ISO／IEC15408，我国也于2001年将CC作为信息评估的国家标准（GB／T18336－2001）发布。
评估标准只提供了评估中应当遵循的准则，并不给出通用的方法和模型。
在实际评估当中，应针对不同的安全评估对象，以评估标准为准则，制定适合于具体情况的方法和模型。
不论是从各种评估标准还是众多信息安全评估模型来看，信息安全评估都是从安全需求出发，结合资产价值对系统的威胁、脆弱性进行全面的考察和评判。
随着互联网的普及和基于网络业务的增加，网络系统的风险评估作为信息安全评估的一个分支已经越来越受到人们的重视。
研究者们已经提出了大量模型和方法，这些方法和模型大部分都是离线的，侧重于各个层次上的系统漏洞评估。
以前由于技术上的限制，针对入侵的实时、在线风险评估方法和模型非常少，随着网络安全技术（特别是各种后入侵检测技术）的发展，使得在线风险评估成为可能，预计在线风险评估将是网络安全领域一个新的研究热点。
在线的网络入侵风险评估与离线的网络风险评估的主要区别在于：·离线网络风险评估的方法关注的焦点是从服务、主机到网络的所有层次存在的漏洞；而在线评估方法焦点在于发生的入侵。
·离线的方法所评估的范围要包含网络系统中的所有单元；而在线评估的范围只限于受到此次入侵所影响到的服务、主机和网络。
·离线评估方法和其得到的评估结果是非实时的、静态的；而在线评估方法和结果是动态的、实时的。
·离线评估往往是对目标潜在风险的评估；而在线评估方法是对正在发生的风险进行评估。
无论是安全事件分级还是在线风险评估，对入侵分析和入侵响应都有重大意义，主要体现在如下几个方面。

编辑推荐

《网络入侵分析与入侵响应》是高等教育“十二五”创新型规划教材之一。

第一图书网, tushu007.com

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