

<<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：9787040242676

10位ISBN编号：7040242672

出版时间：2008-6

出版时间：李剑 高等教育出版社 (2008-06出版)

作者：李剑 著

页数：235

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

《高等学校信息安全系列教材：入侵检测技术》作为信息安全系列教材，全面系统地介绍了信息安全领域主要内容之一的入侵检测技术。

全书内容共分为14章，分别介绍了入侵检测概述、常见的入侵方法与手段、入侵检测系统模型、误用与异常入侵检测系统、模式串匹配与入侵检测、基于主机的入侵检测系统、基于网络的入侵检测系统、典型的入侵检测技术、基于主体的分布式的入侵检测系统、入侵检测系统的相关标准与评估、典型的入侵检测系统、典型的入侵检测产品、使用Snort进行入侵检测以及入侵检测技术的发展。

附录A列出了常用入侵检测术语及其释义；附录B是一个实验，介绍如何在Windows下使用Snort来配置一个网络入侵检测系统。

## 书籍目录

第1章 入侵检测概述1.1 入侵检测简介1.1.1 入侵的定义1.1.2 入侵检测的概念1.1.3 入侵检测的发展历史1.1.4 入侵检测系统的作用1.2 入侵检测系统在信息安全中的地位1.2.1 P2DR2安全模型与入侵检测系统的关系1.2.2 传统安全技术的局限性1.3 入侵检测系统的基本原理与工作模式1.3.1 入侵检测系统的基本原理1.3.2 入侵检测系统的基本工作模式1.4 入侵检测系统的分类1.4.1 根据检测技术分类1.4.2 根据数据来源分类1.4.3 根据体系结构分类1.4.4 根据入侵检测的时效性分类1.5 常用入侵检测方法思考题第2章 常见的入侵方法与手段2.1 信息系统的漏洞2.1.1 漏洞的概念2.1.2 漏洞的具体表现2.1.3 漏洞的分类2.2 信息系统面临的威胁2.3 攻击概述2.3.1 黑客2.3.2 攻击的概念与分类2.3.3 攻击的一般流程2.4 典型的攻击技术与方法2.4.1 预攻击探测2.4.2 口令破解攻击2.4.3 缓冲区溢出攻击2.4.4 欺骗攻击2.4.5 拒绝服务攻击2.4.6 数据库攻击2.4.7 木马攻击思考题第3章 入侵检测系统模型3.1 入侵检测系统模型概述3.2 信息收集3.2.1 信息收集概述3.2.2 信息的来源3.2.3 信息的标准化3.3 信息分析3.3.1 模式匹配3.3.2 统计分析3.3.3 完整性分析3.3.4 数据分析机制3.4 报警与响应3.4.1 被动响应与主动响应3.4.2 主动响应在商业上的应用3.4.3 “蜜罐”技术3.4.4 “蜜网”技术思考题第4章 误用与异常入侵检测系统4.1 误用入侵检测系统4.1.1 误用入侵检测概述4.1.2 误用入侵检测系统的类型4.1.3 误用入侵检测方法4.1.4 误用入侵检测系统的缺陷4.2 异常入侵检测4.2.1 异常入侵检测概述4.2.2 异常入侵检测方法思考题第5章 模式串匹配与入侵检测5.1 模式串匹配算法概述5.2 模式串匹配技术及其在入侵检测中的应用5.3 模式串匹配算法研究现状5.3.1 精确模式串匹配算法5.3.2 近似模式串匹配算法5.4 精确模式串匹配算法概述5.4.1 单模式串匹配算法5.4.2 最简单的单模式串匹配算法——蛮力法5.4.3 KMP算法5.4.4 Boyer-Moore算法5.4.5 BOM算法5.4.6 多模式串匹配算法5.4.7 最简单的多模式串匹配算法——蛮力法5.4.8 Aho-Corasick算法5.4.9 Wu-Manber算法5.4.10 SBOM算法5.5 不同串匹配算法性能对比5.5.1 实验环境描述5.5.2 关键词高频出现时的测试5.5.3 关键词低频出现时的测试5.6 串匹配算法的一些改进思考题第6章 基于主机的入侵检测系统6.1 基于主机的入侵检测系统概述6.2 获取审计数据6.2.1 获取Windows的审计数据6.2.2 获取UNIX的审计数据6.3 基于主机的入侵检测系统模型6.3.1 一种基于主机的入侵检测系统结构6.3.2 入侵特征选取6.3.3 入侵特征预处理6.4 基于主机的入侵检测系统的优缺点6.4.1 基于主机的入侵检测系统的优点6.4.2 基于主机的入侵检测系统的缺点思考题第7章 基于网络的入侵检测系统7.1 基于网络的入侵检测系统概述7.2 基于网络的入侵检测系统模型7.2.1 一种基于网络的入侵检测系统结构7.2.2 网络层7.2.3 主体层7.2.4 分析层7.2.5 管理层7.3 包捕获技术7.3.1 winPcap简介7.3.2 包捕获原理7.3.3 windows下包捕获程序的结构7.3.4 windows下捕获包的主要源代码7.4 基于网络的入侵检测系统的优缺点7.4.1 基于网络的入侵检测系统的优点7.4.2 基于网络的入侵检测系统的缺点思考题第8章 典型的入侵检测技术8.1 概述8.2 基于神经网络的入侵检测技术8.2.1 基于神经网络的入侵检测系统模型8.2.2 系统功能描述8.2.3 系统数据捕获及预处理实现8.2.4 神经网络分类模块实现8.3 基于遗传算法的入侵检测技术8.3.1 遗传算法简介8.3.2 遗传算法在入侵检测系统中的应用8.4 基于数据挖掘的入侵检测技术8.4.1 数据挖掘概述8.4.2 数据挖掘算法8.4.3 入侵检测系统中的特定数据挖掘算法8.5 基于数据融合的入侵检测技术8.5.1 基于数据融合的入侵检测系统介绍8.5.2 基于警报融合的入侵检测系统8.6 基于免疫的入侵检测技术8.7 基于协议分析的入侵检测技术8.7.1 基于协议分析的入侵检测技术概述8.7.2 一种基于马尔可夫链的协议分析入侵检测系统模型8.8 基于入侵容忍的入侵检测技术8.8.1 基于入侵容忍的入侵检测技术概述8.8.2 基于入侵容忍的入侵检测系统模型8.8.3 基于多级门限的入侵容忍安全方案思考题第9章 基于主体的分布式入侵检测系统9.1 基于主体的分布式入侵检测系统的应用背景9.2 基于主体的分布式入侵检测系统的结构9.2.1 分布式入侵检测系统的特征9.2.2 分布式入侵检测系统的体系结构9.2.3 分布式入侵检测体系结构的优点9.2.4 多主体系统简介9.2.5 主体简介9.3 入侵检测系统中的主体实现技术9.3.1 中心主体9.3.2 分析主体9.3.3 主机主体和网络主体9.4 主体之间的通信9.4.1 知识查询和操纵语言9.4.2 消息示例9.4.3 KQML/OWL消息的封装与解析过程9.5 分布式入侵检测系统自身的安全问题思考题第10章 入侵检测系统的相关标准与评估10.1 入侵检测的标准化工作10.1.1 入侵检测工作组10.1.2 公共入侵检测框架10.1.3 国内入侵检测系统标准10.2 入侵检测系统的性能指标10.2.1 性能指标简介10.2.2 影响性能指标的因素10.3 入侵检测系统的测试与评估10.3.1 入侵检测系统的测试步骤10.3.2 评估入侵检测系统的性能指标思考题第11章 典型的入侵检测系统11.1 典型入侵检测系统介绍11.1.1 DIDS11.1.2

## &lt;&lt;入侵检测技术&gt;&gt;

CSM11.1.3 EMERALD11.1.4 AAFID11.1.5 NetSTAT11.1.6 GRIDS11.1.7 IDA11.1.8 MAIDS11.2 总结和分析思考题第12章 典型的入侵检测产品12.1 入侵检测产品概述12.2 典型的入侵检测产品12.2.1 NetRanger12.2.2 CyberCop12.2.3 LinkTrust12.2.4 Dragon Sensor12.2.5 RealSecure12.2.6 Kane Security Monitor12.2.7 OmniGuard/Intruder Alert12.2.8 SessionWall-312.2.9 天阗12.2.10 天眼12.2.11 冰之眼12.3 入侵检测产品选购要点思考题第13章 使用Snort进行入侵检测13.1 Snort概述13.1.1 Snort的工作模式13.1.2 Snort入侵检测概述13.1.3 Snort入侵检测的特点13.2 Snort的体系结构13.3 Snort的规则13.3.1 Snort的规则基础13.3.2 Snort的规则头13.3.3 规则选项13.3.4 预处理器13.3.5 输出模块13.3.6 建立好的Snort规则思考题第14章 入侵检测技术的发展14.1 现有入侵检测技术的局限性14.2 入侵检测技术的发展方向14.2.1 入侵技术的发展14.2.2 入侵检测技术的发展14.2.3 入侵检测新技术14.3 入侵防御系统14.3.1 IPS的概念14.3.2 IPS的功能与特点14.3.3 IPS的优势与局限性14.3.4 IPS的未来发展方向14.4 入侵管理系统14.4.1 IMS对IDS的扩充14.4.2 入侵管理系统对应急响应的支撑思考题附录A 入侵检测常见英语词汇及翻译附录B 在Windows下采用Snort配置入侵检测系统参考文献

<<入侵检测技术>>

编辑推荐

<<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>