

<<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：9787115162335

10位ISBN编号：7115162336

出版时间：2007-5

出版时间：人民邮电

作者：曹元大

页数：226

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

《普通高等教育“十一五”国家级规划教材·21世纪高等院校信息安全系列规划教材：入侵检测技术》全面、系统地介绍了入侵检测的基本概念、基本原理和检测流程，较为详尽地讲述了基于主机的入侵检测技术和基于网络的入侵检测技术，在此基础上介绍了入侵检测系统的标准与评估，并以开源软件snort为例对入侵检测的应用进行了分析。

《普通高等教育“十一五”国家级规划教材·21世纪高等院校信息安全系列规划教材：入侵检测技术》语言通俗，层次分明，理论与实例结合，可以作为高等学校计算机相关专业或信息安全专业本科生高年级的选修课教材，对从事信息和网络安全方面的管理人员和技术人员也有参考价值。

## &lt;&lt;入侵检测技术&gt;&gt;

## 书籍目录

- 第1章 入侵检测概述 1.1 网络安全基本概念 1.1.1 网络安全的实质 1.1.2 网络系统的安全对策与入侵检测 1.1.3 网络安全的P2DR模型与入侵检测 1.2 入侵检测的产生与发展 1.2.1 早期研究 1.2.2 主机IDS研究 1.2.3 网络IDS研究 1.2.4 主机和网络IDS的集成 1.3 入侵检测的基本概念 1.3.1 入侵检测的概念 1.3.2 入侵检测的作用 1.3.3 研究入侵检测的必要性 习题 第2章 入侵方法与手段 2.1 网络入侵 2.1.1 什么是网络入侵 2.1.2 网络入侵的一般流程 2.1.3 典型网络入侵方法分析 2.2 漏洞扫描 2.2.1 扫描器简介 2.2.2 秘密扫描 2.2.3 OS Fingerprint技术 2.3 口令破解 2.3.1 Windows口令文件的格式及安全机制 2.3.2 UNIX口令文件的格式及安全机制 2.3.3 破解原理及典型工具 2.4 拒绝服务攻击 2.4.1 拒绝服务攻击的原理 2.4.2 典型拒绝服务攻击的手段 2.5 分布式拒绝服务攻击 2.6 缓冲区溢出攻击 2.6.1 堆栈的基本原理 2.6.2 一个简单的例子 2.7 格式化字符串攻击 2.8 跨站脚本攻击 2.9 SQL Injection攻击 习题 第3章 入侵检测系统 3.1 入侵检测系统的基本模型 3.1.1 通用入侵检测模型(Denning模型) 3.1.2 层次化入侵检测模型(IDM) 3.1.3 管理式入侵检测模型(SNMP-IDSM) 3.2 入侵检测系统的工作模式 3.3 入侵检测系统的分类 3.3.1 根据目标系统的类型分类 3.3.2 根据入侵检测系统分析的数据来源分类 3.3.3 根据入侵检测分析方法分类 3.3.4 根据检测系统对入侵攻击的响应方式分类 3.3.5 根据系统各个模块运行的分布方式分类 3.4 入侵检测系统的构架 3.4.1 管理者 3.4.2 代理 3.5 入侵检测系统的部署 3.5.1 网络中没有部署防火墙时 3.5.2 网络中部署防火墙时 习题 第4章 入侵检测流程 4.1 入侵检测的过程 4.1.1 信息收集 4.1.2 信息分析 4.1.3 告警与响应 4.2 入侵检测系统的数据源 4.2.1 基于主机的数据源 4.2.2 基于网络的数据源 4.2.3 应用程序日志文件 4.2.4 其他入侵检测系统的报警信息 4.2.5 其他网络设备和安全产品的信息 4.3 入侵分析的概念 4.3.1 入侵分析的定义 4.3.2 入侵分析的目的 4.3.3 入侵分析应考虑的因素 4.4 入侵分析的模型 4.4.1 构建分析器 4.4.2 分析数据 4.4.3 反馈和更新 4.5 入侵检测的分析方法 4.5.1 误用检测 4.5.2 异常检测 4.5.3 其他检测方法 4.6 告警与响应 4.6.1 对响应的需求 4.6.2 响应的类型 4.6.3 按策略配置响应 4.6.4 联动响应机制 习题 第5章 基于主机的入侵检测技术 5.1 审计数据的获取 5.1.1 系统日志与审计信息 5.1.2 数据获取系统结构设计 5.2 审计数据的预处理 5.3 基于统计模型的入侵检测技术 5.4 基于专家系统的入侵检测技术 5.5 基于状态转移分析的入侵检测技术 5.6 基于完整性检查的入侵检测技术 5.7 基于智能体的入侵检测技术 5.8 系统配置分析技术 5.9 检测实例分析 习题 第6章 基于网络的入侵检测技术 6.1 分层协议模型与TCP/IP协议簇 6.1.1 TCP/IP协议模型 6.1.2 TCP/IP报文格式 6.2 网络数据包的捕获 6.2.1 局域网和网络设备的工作原理 6.2.2 Sniffer介绍 6.2.3 共享和交换网络环境下的数据捕获 6.3 包捕获机制与BPF模型 6.3.1 包捕获机制 6.3.2 BPF模型 6.4 基于Libpcap库的数据捕获技术 6.4.1 Libpcap介绍 6.4.2 Windows平台下的Winpcap库 6.5 检测引擎的设计 6.5.1 模式匹配技术 6.5.2 协议分析技术 6.6 网络入侵特征实例分析 6.6.1 特征(Signature)的基本概念 6.6.2 典型特征——报头值 6.6.3 候选特征 6.6.4 最佳特征 6.6.5 通用特征 6.6.6 报头值关键元素 6.7 检测实例分析 6.7.1 数据包捕获 6.7.2 端口扫描的检测 6.7.3 拒绝服务攻击的检测 习题 第7章 入侵检测系统的标准与评估 7.1 入侵检测的标准化工作 7.1.1 CIDEF 7.1.2 IDMEF 7.1.3 标准化工作总结 7.2 入侵检测系统的性能指标 7.2.1 评价入侵检测系统性能的标准 7.2.2 影响入侵检测系统性能的参数 7.2.3 评价检测算法性能的测度 7.3 网络入侵检测系统测试评估 7.4 测试评估内容 7.4.1 功能性测试 7.4.2 性能测试 7.4.3 产品可用性测试 7.5 测试环境和测试软件 7.5.1 测试环境 7.5.2 测试软件 7.6 用户评估标准 7.7 入侵检测评估方案 7.7.1 离线评估方案 7.7.2 实时评估方案 习题 第8章 Snort分析 8.1 Snort的安装与配置 8.1.1 Snort简介 8.1.2 底层库的安装与配置 8.1.3 Snort的安装 8.1.4 Snort的配置 8.1.5 其他应用支撑的安装与配置 8.2 Snort总体结构分析 8.2.1 Snort的模块结构 8.2.2 插件机制 8.2.3 Libpcap应用的流程 8.2.4 Snort的总体流程 8.2.5 入侵检测流程 8.3 Snort的使用 8.3.1 Libpcap的命令行 8.3.2 Snort的命令行 8.3.3 高性能的配置方式 8.4 Snort的规则 8.4.1 规则的结构 8.4.2 规则的语法 8.4.3 预处理程序 8.4.4 输出插件

## <<入侵检测技术>>

8.4.5 常用攻击手段对应规则举例 8.4.6 规则的设计 8.5 使用Snort构建入侵检测系统实例 习题  
第9章 入侵检测的发展趋势 9.1 入侵检测技术现状分析 9.2 目前的技术分析 9.3 入侵检测的先进技术 9.4 入侵检测的前景 9.4.1 入侵检测的能力 9.4.2 高度的分布式结构 9.4.3 广泛的信息源 9.4.4 硬件防护 9.4.5 高效的安全服务 9.4.6 IPv6对入侵检测的影响 习题 附录  
主要入侵检测系统介绍与分析 附1 国外主要入侵检测系统简介 附2 国内主要入侵检测系统简介  
参考文献

<<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>