第一图书网, tushu007.com

<<入侵检测系统及实例剖析>>

图书基本信息

书名：<<入侵检测系统及实例剖析>>

13位ISBN编号：9787302053927

10位ISBN编号：7302053928

出版时间：2002-5-1

出版时间：第1版 (2002年1月1日)

作者：韩东海,王超,李群

页数：278

字数：418

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

本书是一本系统介绍入侵检测系统理论与实际应用的中高级参考用书。
全书分为原理篇、使用篇和分析篇三大部分。
原理篇介绍了入侵检测的基本原理，主要包括面对的威胁、分类检测的方法及其关键技术。
使用篇选取常用的开放源代码系统——Snort和AAFID系统，介绍了系统的总体框架和主要设计思想，
分析篇是本书的重点，结合具体的应用实例对系统的源代码进行逐一剖析，全部源代码完全公开。
本书有助于计算机网络安全从业人员加深对入侵检测的理解，积累技术相关的设计与开发经验，对于广大的程序员提高编程水平也大有裨益，是极佳案头参考用书。
同时也适用于各大专院校计算机专业的教师和高年级学生。

书籍目录

第1篇　入侵检测的原理
第1章　入侵检测相关基本概念
1．l　网络安全基本概念
1．1．l　网络安全的基本观点
l．1．2　PDR模型
1．1．3　入侵检测：在PDR模型中的位置与作用
1．2　我们面对的威胁
1．2．l　攻击来自何方
1．2．2　如何攻击
1．3　什么是入侵检测
1．3．l　概念
1．3．2　入侵检测系统的基本结构
l．4　入侵检测的分类方法学
第2章　基于异常的入侵检测系统
2．l　基于异常的入侵检测
2．2　基于统计学方法的异常检测系统
2．2．1　NIDES的总体结构
2．2．2 NIDES使用的算法
2．3　使用其他的方法进行基于异常的人侵检测
2．4　总结
第3章　基于误用的入侵检测系统
3．l　基本原理
3．1．l　基于误用的入侵检测系统的基本概念
3．1．2　误用检测系统的类型
3．2　误用检测专家系统
3．3　模型推理检测系统
3．4　模式匹配检测系统
3．4．l　模式匹配原理
3．4．2　模式匹配系统的特点
3．4．3　模式匹配系统具体的实现问题
3、5　误用检测与异常检测的比较
第4章　标准及主要入侵检测系统分析
4．l　主要商用入侵检测系统简介
4．1．1　NFR公司的NID
4．1．2 ISS公司的RealSecure
4．l．3 NAI公司的CyberCop Intrusion Protection
4．l．4 Cisco公司的Cisco Secure IDS
4．2　主要非商用系统简介
4．2．1　SRI的NIDES
4．2．2　SRI的EMERALD
4．2．3　CERIAS的ESP
4．2．4　其他一些系统
4．3　入侵检测的标准化工作
4．3．1　CIDF的标准化工作
4．3．2　IDWG的标准化

4．3．3　标准化工作总结
第2篇　常用入侵检测系统的使用
第5章　Snort的安装、配置与使用
5．l　接触Snort
5．1．1　Snort简介
5．1．2　如何获取Snort
5．2　底层库的安装与配置
5．2．1　Snort所需的底层库
5．2．2　底层库的安装
5．3　Snort的安装与配置详解
5．3．1　Snort的安装
5．3．2 Snort的配置
5．3．3　其他应用支撑的安装与配置
5．4　Snort使用详解
5．4．1　Libpcap的命令行
5．4．2 Snort的命令行
5．4．3　高性能的配置方式
第6章　Snort的规则
6．l　规则的语法
6．1．l　规则文件的语法
6．1．2　规则头
6．1．3　规则选项
6．1．4　预处理器
6．1．5　输出模块
6．2　常用攻击手段对应的规则举例
6．3　如何设计自己的规则
第7章　AAFID的安装、配置与使用
7．l　接触 AAFID
7．1．1　AAFID简介
7．1．2　如何获取 AAFID
7．2　Perl的安装
7．2．1　Perl的安装
7．2．2　所需Perl模块的安装
7．3　AAFID的安装与配置
7．3．1　AAFID的安装
7．3．2　AAFID的配置
7．4 AAFID使用详解
7．4．1　AAFID命令行的使用方式
7．4．2　AAFID的图形界面使用方式
第8章　AAFID的代理与过滤器
8．1　AAFID的规则：没有规则
8．1．1　AAFID系统的代理
8．l．2　AAFID系统的过滤器.
8．2　代理的编写
8．2．l　编写代理的基本步骤
8．2．2　简单代理编写实例
8．3　过滤器的编写

8．3．l　一般原则
8．3．2　实例说明
第3篇　源代码分析
第9章　Snort总体结构分析
9．l　总体结构
9．1．1　Snort的模块结构
9．l．2　Snort的源代码布局
9．1．3　插件机制
9．2　Snort的总体流程
9．2．l　通常libpcap应用的流程
9．2．2 Snort的总体流程
9．2．3　入侵检测流程
第10章 Snort关键模块剖析
10．l　主控模块
10．1．l　主控流程分析
10．1．2　插件管理分析
10．1．3　全局变量
10．2　规则模块
10．2．1　Snort规则语法树的生成
10．2．2 Snort规则检测的实现
10．3　解码模块
10．3．l　数据结构分析
10．3．2　函数分析
10．4　处理模块
10．4．l　处理模块的内容
10．4．2　处理模块的基本架构
10．4．3　处理模块详细介绍
10．5　预处理模块
10．5．l　预处理模块的内容
10．5．2　预处理模块的基本架构
10．5．3　预处理模块详细介绍
10．6　输出模块
10．6．l　输出模块的内容
10．6．2　输出模块的基本架构
10．6．3　输出模块详细介绍
10．7　日志模块
10．7．l　日志模块的内容
10．7．2　日志模块详细介绍
10．8　辅助模块
10．8．l　辅助模块的内容
10．8．2　辅助模块功能分析
第11章　AAFID总体结构分析
11．1　AAFID的总体结构
11．1．1　AAFID系统源代码简单说明
11．1．2　AAFID系统的类层次结构
11．1．3 AAFID系统主要模块
11．2 AAFID的总体流程

11．2．1　AAFID系统的事件机制
11．2．2 AAFID系统中实体的运行模式
11．2．3 AAFID系统的典型流程
第12章　AAFID关键模块剖析
12．l　基础功能模块
12．l．1　Entity类
12．1．2 ControllerEntity类
12．1．3 Filter类
12．1．4 Agent类
12．2　过滤功能模块
12．3　代理功能模块
12．4　监视器模块
12．4．l　连接处理
12．4．2　实体请求处理
12．4．3　实体管理
12．5　收发器模块
12．6　运行管理模块
12．6．l　事件处理
12．6．2　启动器
12．7　消息处理模块
12．7．l　格式定义及标准消息
12．7．2　消息处理函数
12．8　日志管理模块
12．8．l　主题管理Topics．pm
12．8．2　日志管理Log．pm
12．9　通信处理模块
12．9．l　输出功能
12．9．2　输入功能
12．9．3　辅助功能
12．10　配置管理模块
12．10．1　Tags．pm
12．10．2 Config．pm
12．11　图形界面模块
12．12　辅助模块
12．12．l　通用功能Common类
12．12．2　常量管理Constants类
12．12．3　队列管理FiniteQueue类与NumQueue类
12．12．4　系统相关性管理System类
后记
附录A　术语
附录B　函数及结构索引
附录C　参考文献

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