
基于入侵检测的并行网络安全系统的设计与实现

摘 要

本文通过研究入侵检测技术及模式匹配算法,提出一种分级嵌套精确串匹配算法,并结合此算法实现一种树状结构的网络安全体系架构以及单节点网络安全系统。具体研究如下:

(1)入侵检测系统架构研究。对 IDS 的相关技术进行深入研究,提出一种高效的分布式并行 IDS 系统架构及安全策略,并给出了单一结点网络安全系统的设计思路。

(2)子网结点网络安全系统的研究与实现。研究并实现流过滤系统、并行入侵检测系统以及数据统计系统。其中双链层分级嵌套算法用于流过滤系统中过滤器设计,并行双链层分级嵌套算法用于 DIDS 中数据分析器的设计。

(3)分别对由 KMP、BM 以及改进算法实现的数据分析器进行实验验证,证明以改进算法的高效可行性。

关键词: 入侵检测; 模式匹配; MPI; 流过滤; DIDS

论文类型: 应用研究

目 录

1 绪论	1
2 入侵检测技术概述.....	2
2.1 网络入侵.....	2
2.2 入侵检测系统架构.....	2
2.3 入侵检测系统的分类.....	3
3 DIDS 系统架构及安全策略研究.....	4
3.1 相关技术介绍.....	4
3.2 DIDS 总体架构设计	4
3.2.1 树状分层结构的 DIDS 设计思路	4
3.2.2 DIDS 的结点注册	5
3.2.3 DIDS 的通信机制	6
3.2.4 DIDS 的运行实例	7
3.3 DIDS 子网结点架构设计	8
3.3.1 结点的网络安全系统设计思路	8
3.3.2 流过滤器的结构设计.....	9
3.3.3 并行 DIS 系统结构设计.....	9
3.3.4 数据统计系统设计.....	12
4 网络安全系统的实现.....	14
4.1 相关技术要点.....	14
4.1.1 原始套接字编程.....	14
4.1.2 Winpcap 编程	14
4.2 流过滤系统设计实现.....	14
4.2.1 基于原始套接字的 Win32 编程实现.....	14
4.2.2 基于 Winpcap 的 MFC 编程实现.....	16
4.3 入侵检测系统设计实现.....	19
4.3.1 数据采集器设计	19
4.3.2 数据分析器设计	19
4.3.3 管理平台设计	20

4.4 数据统计系统设计实现.....	24
5 总结	26
致谢	27
参考文献	28
网络学院毕业论文独创性声明	29

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要
下载或阅读全文，请访问：

<https://d.book118.com/705230322112011310>