计算机工程与应用 2005下 (35期): ISSN: 1002-8331 CN: 11-2127/TP

网络、通信与安全

（50元）（935元）滥用和异常技术相结合的分布式入侵检测系统的设计与实现

张云鹏, 胡飞, 马春燕, 陆伟, 李梅

西北工业大学软件学院

收稿日期 2004-12-7 修回日期 网络版发布日期 接受日期

摘要 本文设计并实现了一个入侵检测系统－SC-IDS，该系统采用滥用和异常相结合的检测方法，分布式的体系结构，符合P2DR模型。克服了传统系统的缺点，如，误警率和漏警率高、可扩展性弱、不能适应大规模网络、不能与其它安全产品协同工作等。在实际应用中取得了良好效果。

关键词 入侵检测,设计,网络安全,防火墙,防病毒技术

分类号

Design and Implementation of Distributed Intrusion Detection System Based on Combines Knowledge and Anomaly Technique

,Fei Hu,,,

西北工业大学软件学院

Abstract

The author has established and accomplished the intrusion detection system—SC-IDS in the thesis. It combines the knowledge-based IDS and anomaly-based IDS into a system,it accord with P2DR model and the distributed framework. It surmount the shortcoming of traditional ways of detection, for example, high false positive and false negative rate; can’t adapt large-scale network; can’t coordinated work with other security product etc. It gains a good effect after operation.

Key words Intrusion Detection Design Network Security Firewall Anti－virus

DOI:

通讯作者 张云鹏 poweryp poweryp poweryp@163.com