现代图书情报技术 2007 (1): 44-48 ISSN: 1003-3513 CN: 11-2856/G2

20届机检会论文选登

网络蠕虫检测系统的设计和实现

钱旭[1];顾巍[1];陈凌晖[1];丁晓峰[1;2]

北京文献服务处[1]

收稿日期 2006-10-13 修回日期 网络版发布日期 2007-1-24 接受日期

摘要 设计一种面向实际应用的网络蠕虫检测系统，并初步实现原型系统。该系统采用分布式架构，主要针对局域网内的未知蠕虫进行实时监控，通过分析网络数据流量，提取蠕虫传播过程中的普遍特征，预测未知蠕虫在网内大规模爆发的趋势。该蠕虫检测系统可作为网络安全体系的重要组成部分，保障本地网络系统的稳定、安全运行。

Abstract The application system for network worm detecting is designed, as well the prototype is constructed. The distributed structure is adopted to monitor the unknown worms at real-time, analyse the network stream, bring up the signature of worm spreading to identify that the unknown worms erupt in local network. The worm detection system could be applied as a significant aspect of network security architecture to secure the local network system.

关键词 网络蠕虫 分布式架构 异常检测

Key words Network worm;Distributed structure;Anomaly detection

分类号 TP309.5

DOI:

通讯作者:
钱旭 qx@cetin.net.cn
作者个人主页: 钱旭 顾巍 陈凌晖 丁晓峰