

安全技术

基于Agent的分布式协作入侵检测系统

林昭文, 赵毅德, 马 严

(北京邮电大学计算机科学与技术学院, 北京 100876)

收稿日期 修回日期 网络版发布日期 2008-2-29 接受日期

摘要 分析了当前入侵检测系统及其存在的问题, 提出一个基于Agent的分布式协作检测模型(ADCM), 给出其原型系统。该模型通过逻辑检测域(LDD)之间的协作通信, 完成对新型分布式攻击的检测。实验证明ADCM可以有效地检测出具有一定隐蔽性的、分布式的协作攻击。

关键词 [入侵检测](#) [分布式攻击](#) [代理](#) [协作模型](#)

分类号 [TP393](#)

DOI:

通讯作者:

作者个人主页: [林昭文](#); [赵毅德](#); [马 严](#)

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF \(159KB\)](#)
- ▶ [\[HTML全文\]\(0KB\)](#)
- ▶ [参考文献\[PDF\]](#)
- ▶ [参考文献](#)

服务与反馈

- ▶ [把本文推荐给朋友](#)
- ▶ [加入我的书架](#)
- ▶ [加入引用管理器](#)
- ▶ [引用本文](#)
- ▶ [Email Alert](#)
- ▶ [文章反馈](#)
- ▶ [浏览反馈信息](#)

相关信息

- ▶ [本刊中 包含“入侵检测”的 相关文章](#)
- ▶ 本文作者相关文章
 - [林昭文, 赵毅德, 马 严](#)