

博士论文

基于粗糙集理论的网络型入侵检测系统

张红梅^{1,2}, 王 勇^{1,2}, 王行愚¹

(1. 华东理工大学信息学院, 上海200237; 2. 桂林电子工业学院网络信息中心, 桂林541004)

收稿日期 修回日期 网络版发布日期 2006-9-25 接受日期

摘要 为解决目前大多数入侵检测产品或模型对未知攻击的检测都存在精度低或者虚警率高的问题, 建立了一个基于网络的入侵检测实验平台, 使用了多种新的攻击工具实施攻击; 并在此基础上提取了网络连接的29项实时特征; 应用粗糙集理论实现了一个网络连接的检测器。经实验表明, 所选取的网络连接特征能较好地反映网络安全状况, 粗糙集理论应用于多类分类问题和未知攻击的检测方面是有效的。

关键词 [入侵检测系统](#) [粗糙集](#) [不可分辨关系](#) [离散化](#) [数据约简](#)

分类号 [TP393](#)

DOI:

通讯作者:

作者个人主页: [张红梅^{1,2}](#); [王 勇^{1,2}](#); [王行愚¹](#)

扩展功能

本文信息

▶ [Supporting info](#)

▶ [PDF](#) (189KB)

▶ [\[HTML全文\]](#) (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“入侵检测系统”的相关文章](#)

▶ 本文作者相关文章

• [张红梅^{1,2}](#), [王 勇^{1,2}](#), [王行愚¹](#)