

安全技术

基于HMM和STIDE的异常入侵检测方法

孙彦, 李永忠, 罗军生

(江苏科技大学电子信息学院, 镇江 212003)

收稿日期 修回日期 网络版发布日期 2008-2-1 接受日期

**摘要** 入侵检测是对正在发生或已经发生的入侵行为的一种识别过程。异常检测是入侵检测的主要分析方法之一。该文在传统的使用单一入侵检测算法的基础上, 提出一种基于HMM和STIDE复合算法的异常入侵检测方法。HMM和STIDE复合算法被用来区分未知的行为是合法操作还是一次入侵。实验证明该方法具有低虚警率和高检测率。

**关键词** [入侵检测](#) [异常检测](#) [HMM方法](#) [STIDE方法](#)

**分类号** [TP393](#)

**DOI:**

通讯作者:

作者个人主页: [孙彦](#); [李永忠](#); [罗军生](#)

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF](#) (99KB)
- ▶ [\[HTML全文\]](#) (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
  - [孙彦, 李永忠, 罗军生](#)