计算机工程 2008 34 (2): 1-3 ISSN: 1000-3428 CN: 31-1289/TP 首页 当期目录 上一期 下一期

博士论文

# 基于系统调用和数据挖掘的程序行为异常检测

田新广1,2，邱志明1，李文法2,3，孙春来2，段洣毅2,3

田新广1,2，邱志明1，李文法2,3，孙春来2，段洣毅2,3

收稿日期 修回日期 网络版发布日期 2008-1-4 接受日期

摘要 异常检测是目前入侵检测研究的主要方向之一。该文提出一种新的程序行为异常检测方法，主要用于Linux或Unix平台上以系统调用为审计数据的入侵检测系统。该方法利用数据挖掘技术中的序列模式对特权程序的正常行为进行建模，根据系统调用序列的支持度和可信度在训练数据中提取正常模式。在检测阶段，通过序列模式匹配对被监测程序的行为异常程度进行分析，提供两种可选的判决方案。实验结果表明，该方法具有良好的检测性能。

关键词 入侵检测 异常检测 系统调用 数据挖掘

分类号 TP393

**DOI:**

通讯作者:

作者个人主页: 田新广1;2;邱志明1;李文法2;3;孙春来2;段洣毅2;3