计算机应用 2007 27 (09): 2177-2179 ISSN: 1001-9081 CN: 51-1307/TP

信息与网络安全

攻击案例综合学习系统研究

咎鑫[1];郑庆华[2];范宇倩[2];韩九强[2]

西安交通大学电信学院综合自动化所[1]

收稿日期 2007-3-13 修回日期 网络版发布日期 2007-8-27 接受日期

摘要 随着入侵检测系统在安全领域的广泛应用，入侵报警学习和分析已经成为一个研究热点。针对目前入侵报警泛滥和知识贫乏等问题，设计了一个完整的攻击案例学习系统框架。该学习系统分为两个阶段：入侵报警精简和典型攻击案例挖掘。前者利用改进的密度聚类方法实现相似报警聚合以及报警聚类的自动精简表示，后者利用序列模式挖掘方法挖掘频繁入侵事件序列。进一步提出一种基于入侵执行顺序约束关系的攻击案例评估算法实现典型攻击案例的自动筛选。最后，利用真实入侵报警数据测试了该攻击案例学习系统，结果表明该系统能够实现高效报警精简和典型攻击案例的准确学习。

Abstract With the widespread deployment of Intrusion Detection Systems (IDS) in network security community, intrusion alert learning and analysis has increasingly become an active research area. Due to some problems such as alert flooding and lack of knowledge about attack scenario etc, a comprehensive attack case learning system composed of two learning phases: similar alerts aggregation and typical attack instance learning was presented. Firstly, an improved density-based clustering algorithm was introduced to aggregate huge volume of similar alerts to numbers of alert clusters. Secondly, some representative alerts were chosen to represent the overall alert clusters according to some reduction rules. Eventually, sequence pattern mining approach is used to mine frequent intrusive incidents. Furthermore, an evaluation approach based on execution ordering of attacks was proposed to identify valuable attack instances from frequent sequences of intrusive incidents. A real intrusion alert dataset was used to test our learning system. The experimental results show that our learning system can not only effectively reduce the large amount of alerts but also correctly learn the valuable attack cases.

关键词 入侵检测 密度聚类 序列模式挖掘 攻击案例

Key words Intrusion Detection;Density-based Clustering Algorithm;Sequence Pattern Mining;Attack Case

分类号

DOI:

通讯作者:
咎鑫 zanxin@mail.xjtu.edu.cn;xzan@sei.xjtu.edu.cn

作者个人主页: 咎鑫 郑庆华 范宇倩 韩九强