电子与信息学报 2007 29 (9): 2248-2251 ISSN: 1009-5896 CN: 11-4494/TN

论文

TCP/IP审计数据缩减技术在入侵检测中的可行性研究

田俊峰, 王惠然, 傅 玥

河北大学网络技术研究所 保定 071002

收稿日期 2005-12-16 修回日期 2007-5-21 网络版发布日期 2008-1-25 接受日期

摘要
目前的一些入侵检测系统是利用网络层的TCP/IP数据包里的特征进行分析建模，但TCP/IP的特征属性对检测过程的贡献不同，因而如果能够在不影响检测准确性的前提下，适当缩减特征属性的数量，那么对于提高IDS的检测率和实时性势必产生有益的影响，鉴于此该文提出基于决策树的规则统计方法(DTRS)来缩减TCP/IP的特征属性。它的基本思想是通过在n个子数据集上建立n棵决策树，提取其中的规则，根据特征属性使用频度的不同，计算出相对重要的属性，并通过实验验证了其可行性和有效性。

关键词 入侵检测 特征缩减 决策树

分类号 TP393.08

Research on the Feasibility of TCP/IP Feature Reduction for Intrusion Detection

Tian Jun-feng, Wang Hui-ran, Fu Yue

Institute of Network Technology, Hebei University, Baoding 071002, China

Abstract
At present some Intrusion Detection Systems (IDS) use the features of TCP/IP data packets for analysis and modeling, but due to the different contribution of TCP/IP features to the detecting process a favorable impact may be made on the promotion of IDS's detecting rate and real time if the quantity of properties can be reduced properly without affecting the precision of detection. Therefore, a Decision Tree Rule-based Statistical method (DTRS) in light of this is presented to reduce TCP/IP features. Its primary concept is to create n decision trees in n data subsets, extract the rules, work out the relatively important features in accordance with the frequency of use of different features and verify its feasibility and effectiveness through tests.

Key words Intrusion detection Feature reduction Decision tree

DOI:

通讯作者

作者个人主页 田俊峰; 王惠然; 傅 玥