电子与信息学报 2006 28 (11): 2162-2166 ISSN: 1009-5896 CN: 11-4494/TN

论文

基于误用和异常技术相结合的入侵检测系统的设计与研究

田俊峰, 张 喆, 赵卫东

河北大学数学与计算机学院 保定 071002

收稿日期 2005-3-8 修回日期 2005-9-26 网络版发布日期 2007-11-15 接受日期

摘要
目前，入侵检测系统(IDS) 的漏报率和误报率高一直是困扰IDS用户的主要问题，而入侵检测系统主要有误用型和异常型两种检测技术，根据这两种检测技术各自的优点，以及它们的互补性，将两种检测技术结合起来的方案越来越多地应用于IDS中。该文提出了基于统计的异常检测技术和基于模式匹配的误用检测技术相结合的IDS模型，减少了单纯使用某种入侵检测技术时的漏报率和误报率，从而提高系统的安全性。

关键词 入侵检测系统 异常检测 误用检测 模式匹配 统计分析

分类号 TP393.08

The Design and Research of Intrusion Detection System Based on Misuse and Anomaly

Tian Jun-feng, Zhang Zhe, Zhao Wei-dong

College of Computer and Mathematics, Hebei University, Baoding 071002, China

Abstract
Currently, the false positive and the false negative of Intrusion Detection System are very high. It was always the main problem that bothered the user of IDS. But there are tow main technologies applied in IDS. To this problem, because both the technologies have its own advantages and they can supply for each other. So IDS combined with the tow technologies was used more and more widely. This paper presented a model of IDS based on combination of misuse detection and anomaly detection. In this model, misuse detection is based on pattern matching and Anomaly Detection is based on statistical analysis. It combined the tow technologies to reduce the false positive rate and the false negative rate in only one detection technology, and then to improve security of IDS.

Key words Intrusion Detection System (IDS) Anomaly detection Misuse detection Pattern matching Statistical analysis

DOI:

通讯作者

作者个人主页 田俊峰; 张 喆; 赵卫东