高可用性网络入侵预警方法的改进研究

龚健虎
（广东培正学院 计算机科学与工程系，广东 广州 510800）

摘 要： 高可用性网络通常会受到海量恶意入侵，当前预警方法只能对历史与当前的网络入侵情况进行分析，无法预测未来高可用性网络的入侵情况，为了提高预警精度，提出一种新的高可用性网络入侵预警改进方法，介绍了隐马尔可夫模型，在此基础上，构建依据 HMM 模型的实时高可用性网络入侵预警模型，依据危险理论对评估结果进行分析，将高可用性网络状态划分成四个等级，通过构建的 HMM-NSSP 模型实现网络入侵预警.为了提高 HMM-NSSP 模型的预警精度，引入最大熵法对高可用性网络安全态势进行一致性判定，完成高可用性网络入侵预警方法的改进，实验结果表明，所提方法预警结果和实际结果基本一致，具有很高的预警精度，可用性很高.

关键词： 高可用性网络；入侵；预警

High Availability Network Intrusion Early Warning Method Improvement Research

GONG Jian-hu
(Computer Science and Engineering Department, Guangdong Peizheng College, Guangzhou 510800,China)

Abstract： High availability network usually are a huge number of malicious invasion of current early warning method can only analyze the history and the current network intrusion status, cannot predict the future high availability network invasion situation, in order to improve the accuracy of early warning, put forward a new high availability network intrusion early warning method, this paper introduces the hidden markov model, on this basis, the building based on the HMM model of real-time high availability network intrusion early warning model, according to the analysis of risk theory to the evaluation result, the high availability network state was divided into four grades, by building the HMM - NSSP model to realize the network intrusion early warning. In order to improve the early warning of the HMM- NSSP model precision, the introduction of the maximum entropy method for high availability network security situational consistency judgement, to complete the high availability of network intrusion early warning method improvement, the experimental results show that the proposed method the early warning results and actual results are basically identical, has the very high accuracy of early warning, a high availability.

Key words： high availability network; Invasion; warning

作者简介：
龚健虎 男，（1967-），博士，讲师.研究方向为数据库与知识库和数据挖掘.
E-mail：gongtiger@21cn.com