电子与信息学报 2007 29 (11): 2580-2584 ISSN: 1009-5896 CN: 11-4494/TN

论文

基于shell命令和Markov链模型的用户行为异常检测

田新广[①②],孙春来[①],段洣毅[①]

[①]北京交通大学计算技术研究所 北京 100029;[②]国防科技大学电子科学与工程学院 长沙 410073

收稿日期 2006-4-3 修回日期 2006-9-26 网络版发布日期 2008-2-28 接受日期

摘要
异常检测是目前入侵检测系统(IDS)研究的主要方向。该文提出一种基于shell命令和Markov链模型的用户行为异常检测方法，该方法利用一阶齐次Markov链对网络系统中合法用户的正常行为进行建模，将Markov链的状态与用户执行的shell命令联系在一起，并引入一个附加状态；Markov链参数的计算中采用了运算量较小的命令匹配方法；在检测阶段，基于状态序列的出现概率对被监测用户当前行为的异常程度进行分析，并提供了两种可选的判决方案。文中提出的方法已在实际入侵检测系统中得到应用，并表现出良好的检测性能。

关键词 入侵检测 shell命令 Markov链 异常检测 行为轮廓

分类号 TP393

Anomaly Detection of User Behaviors Based on Shell Commands and Markov Chain Models

Tian Xin-guang[①②], Sun Chun-lai[①], Duan mi-yi[①]

[①]Research Institute of Computing Technology, Beijing Jiaotong University, Beijing 100029, China;
[②]College of Electronic Science and Engineering, National Univ. of Defense Technology, Changsha 410073, China

Abstract
Anomaly detection acts as one of the important directions of research on Intrusion Detection Systems(IDSs).This paper presents a new method for anomaly detection of user behaviors based on shell commands and Markov chain models. The method constructs a one-order Markov chain model to represent the normal behavior profile of a network user, and associates shell commands with the states of the Markov chain. The parameters of the Markov chain model are estimated by a command matching algorithm which is computationally efficient. At the detection stage, the probabilities of the state sequences of the Markov chain is firstly computed, and two different schemes can be used to determine whether the monitored user's behaviors are normal or anomalous while the particularity of user behaviors is taken into account. The application of the method in practical intrusion detection systems shows that it can achieve high detection performance.

Key words Intrusion detection Shell command Markov chain Anomaly detection Behavior profile

DOI:

通讯作者

作者个人主页 田新广[①②];孙春来[①];段洣毅[①]