计算机工程与应用 2008 44 (18): 109-112 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

基于Windows Native API序列的系统行为入侵检测

朱莺嘤[1], 叶 茂[1], 刘乃琦[1], 李 筝[2], 郑凯元[1]

1.电子科技大学 计算机学院，成都 610054

2.电子科技大学 通信学院，成都 610054

收稿日期 2007-9-19 修回日期 2007-11-30 网络版发布日期 2008-6-16 接受日期

摘要 针对Windows系统入侵检测的不足，研究并借鉴Linux下基于系统调用序列进行入侵检测的方法，提出一种采用BP神经网络算法对Windows Native API序列学习和分类的内核级主机入侵检测方案。通过实验，验证了采用Windows Native API序列进行系统入侵的可行性。Native API是Windows系统内核模式下的API，可以类比于Linux下的系统调用。通过训练神经网络学习Native API序列，建立一个对正常和异常Native API序列进行分类的BP神经网络。在入侵检测时，利用训练后的神经网络对不断出现的Windows Native API 序列进行分类，判断系统是否出现异常入侵。

关键词 入侵检测 Windows Native API BP神经网络

分类号

Host intrusion detection based on sequence of Windows Native API

ZHU Ying-ying[1],YE Mao[1],LIU Nai-qi[1],LI Zheng[2],ZHENG Kai-yuan[1]

1.College of Computer，University of Electronic Science and Technology of China，Chengdu 610054，China

2.College of Communication and Inf. Eng.，University of Electronic Science and Technology of China，Chengdu 610054，China

Abstract

Considering the shortcomings of Windows system intrusion detection and the advantages of the Linux system intrusion detection based on the sequence of the system call，a kernel-level host intrusion detection program based on the BP neural network algorithm to study and classify the sequence of Windows Native API is proposed in this paper.Experiment results prove that the sequence of Native API can be used for intrusion detection.Windows Native API means the kernel model API，which is similar to the Linux system call.The neural network is trained to learn the normal and abnormal sequence of Native API.In the intrusion detection，use the trained neural network to classify the emerging Native API sequence，and find whether the intrusion happens.

Key words intrusion detection Windows Native API BP neural network

DOI:

通讯作者 朱莺嘤 zy.2@163.com

扩展功能

本文信息

- Supporting info
- PDF(769KB)
- [HTML全文](0KB)
- 参考文献

服务与反馈

- 把本文推荐给朋友
- 加入我的书架
- 加入引用管理器
- 复制索引
- Email Alert
- 文章反馈
- 浏览反馈信息

相关信息

- 本刊中 包含“入侵检测”的相关文章
- 本文作者相关文章
  - 朱莺嘤
  - 叶 茂
  - 刘乃琦
  - 李 筝
  - 郑凯元