基于数据挖掘的数据库入侵检测的设计与实现

Design and implementation of Database intrusion Detection based on data Mining

摘要

近年来,互联网技术不断发展,对人们的生活产生了巨大影响。但是由于互联网具有很大的复杂性,各式各样的网络问题不断出现。很多组织机构将其数据库连接到网络数据库,这些数据库中有许多隐私数据，这些数据容易被非法分子进行攻击。随着不法分子对数据库入侵技术的不断研究分析，数据库的安全性得不到保障。为了能够应对对数据库的非法入侵，通过对数据的检测以保证数据库中数据的安全，入侵检测系统应运而生。

本文对数据库安全机制进行了分析和研究,对传统的数据库中所应用的关于数据库、入侵检测技术方面的内容进行了介绍。然后对数据挖掘技术作了简要说明，并将其应用到入侵检测系统中。接着结合实际设计了基于数据挖掘的数据库入侵检测系统。本文设计的数据库入侵检测系统通过五个功能模块设计保证了对数据的有效检测,即对数据采集与预处理、数据挖掘、规则匹配、入侵检测和响应单元详细设计,实现了对数据库数据的收集和处理;采用了异常和误用检测的算法混合引擎,对数据的入侵检测效率进行了提升；采用被动式响应方式实现了入侵检测响应。

关键词：数据库安全，数据挖掘，入侵检测

Abstract

In recent years, with the rapid development of Internet technology, Internet devices and computers are widely used in society, which has a great impact on people's lives. However, due to the great complexity of the Internet, a variety of network problems continue to appear. Many organizations connect their databases to network databases, which contain a lot of private data that are vulnerable to attacks by criminals. With the continuous research and analysis of database intrusion technology, the security of database can not be guaranteed. As a security defense measure that can detect, audit and record illegal intrusion from outside and inside the network, intrusion detection system arises at the historic moment.

This paper analyzes and studies the database security mechanism, studies the defects of the traditional database security mechanism, and introduces in detail the contents of database, data mining and intrusion detection technology. This paper describes the application of data mining and intrusion detection in database, and designs a database intrusion detection system based on data mining. The database intrusion detection system designed in this paper can be divided into five modules: data acquisition and processing, data mining, rule matching, intrusion detection and response unit. The algorithm hybrid engine of anomaly and misuse detection is used to improve the efficiency of data intrusion detection, and the passive response mode is used to realize the intrusion detection response.

Keywords: Data mining, database, intrusion detection