Journal of Web Systems and Applications (2021) 3: 17-21
Clausius Scientific Press, Canada
DOI: 10.23977/jwsa.2021.030104
ISSN 2560-6913

Network Security Evaluation and Optimal Active Defense Based on Data Mining Technology

Wenwen Zhao

Hotan Normal College, Hetian, Xinjiang 848000, China

841342198@qq.com

Keywords: Data mining technology, Network security evaluation, Network defense, Computer network, Big data

Abstract:Network security evaluation network security evaluation is a network security technology that judges the behavior of illegal users invading and legal users abusing resources through real-time collection and analysis of key information in computer network and host system, and makes appropriate response. It is another security measure after data encryption, firewall and other measures, With the continuous development of computer network technology, the data to be analyzed expands rapidly. How to improve the detection efficiency has become a top priority, and data mining is a good medicine to solve this problem. Firstly, this paper introduces the related concepts of network security evaluation and data mining, and then analyzes the advantages and disadvantages of the network security evaluation system using data mining technology, Finally, some directions of network defense are put forward.

1. Introduction

With the rapid development of information technology and the increasing needs of human social life, computer and Internet technology can be continuously innovated and developed. With the continuous emergence and development of computer virus, intrusion, attack and other means threatening information security, the problem of computer security is becoming more and more serious [1]. The network security evaluation system is a useful supplement to the firewall. The network security evaluation can detect the attack before the intrusion attack endangers the system, and use the alarm and protection system to expel the attack [2]. Traditionally, companies generally use firewall as the first line of defense for security, and network security evaluation. However, network security evaluation, firewall knowledge is a passive and defensive network security tool. Only using firewall is not enough. Firstly, intruders can find the loopholes of firewall network security evaluation, network security evaluation and bypass the firewall to attack; Secondly, the firewall is powerless against the internal attacks from the network security evaluation [3]. For the above mentioned problems, a more effective solution is the network security evaluation system. The network security evaluation system mainly monitors the use of network security evaluation, system status, behavior network security evaluation and system network security evaluation to detect the unauthorized use of system users and the attempt of intruders outside the system to invade the system by using the security defects of the system [4]. The system can make up for the deficiency

of firewall, provide real-time network security evaluation for the network, and take corresponding protection measures. Network security evaluation system is considered to be the second security gate behind the firewall. The first important problem faced by the network-based network security evaluation system is to effectively deal with massive network data and find suspicious data [5]. In the face of massive data, traditional data analysis tools can only process some surface data, but can not obtain the internal relationship and implicit information between data [6]. As a new thinking method and technical means for large-scale data processing, data mining has developed rapidly in recent years. Therefore, more and more network security evaluation systems have been combined with data mining technology.

2. Network Security Evaluation Data Mining

2.1 Overview of Data Mining

With the trend of big data sweeping the world, the amount of data is increasing exponentially, and the prospect of data mining is bright. At present, data analysis and data application are still in the primary stage, and the market potential of data mining is huge. Through data understanding and data preparation, data analysis, modeling and evaluation, the best algorithm is combined with advanced data analysis and the best algorithm, and finally applied to the field of network security [7]. Data mining is different from traditional data analysis. It is not only limited to understanding the historical and current valuable information, but also pays more attention to the prediction of the future. It carries out in-depth mining through artificial intelligence, machine learning and statistics, mines valuable information from massive data, and filters, collects, arranges, stores, analyzes and uses data. Collect timely, correct, reliable and high-quality data from complex and diverse information data for data analysis, and release the value hidden in the data. Find valuable knowledge rules, mine unknown information, automatically complete mathematical modeling, directly deduce conclusions, and apply the results to network security evaluation [8].

2.2 Introduction of Data Mining

Data mining was originally a technology in database, also known as knowledge discovery in database. Database knowledge discovery technology usually includes the following steps: the first is the data preparation stage, which mainly completes the subtasks of data selection, preprocessing and data transformation, the second is data mining, and the third is result analysis and evaluation [9]. Data mining is one of the steps, and it is the most critical processing step. In the process of data mining, the first thing is to clarify the task and purpose of mining, that is, to establish the model category obtained after data processing; The second is to determine the mining algorithm based on the characteristics of mining data and the needs of users and systems. The main factors that determine the quality of data mining are the quality and scale of data volume and the effectiveness of data mining technology [10]. If the data attribute you choose is inappropriate or the range is incorrect, the mining quality is not satisfactory.

Data mining is to extract the knowledge that people are interested in from a large database. The extracted knowledge can generally be expressed in the form of concepts, rules, laws and patterns. For the network security evaluation system, it is also necessary to extract intrusion features from a large amount of data [11]. The data source of network security evaluation contains a large number of audit records, and most of the audit records are stored in the form of files. It is not enough to rely solely on manual methods to find abnormal phenomena in the records, and the operation is also very inconvenient for network security evaluation. Therefore, the powerful analysis method of data mining can be used for the modeling of network security evaluation [12].

Association rules and sequence rules can be mined by using the relevant algorithms in data mining to analyze the association and sequence of audit data. Through this method, the administrator no longer needs to manually analyze and write the intrusion mode, nor need to guess its feature items by experience when establishing the normal use mode, which has good scalability and adaptability [13].

3. Introduction to Network Security Evaluation

Network security evaluation system is a computer system (which can be composed of software or hardware) to complete the task of network security evaluation. It is a reasonable supplement to traditional defense technologies such as firewall and the second defense system after firewall [14]. It monitors the network without affecting the network performance, so as to provide protection against internal attacks Real time protection against external attacks and misoperation. It takes detection and control as the technical means, plays the role of active defense, and is an indispensable part of network security. In the network security system, the network security evaluation system is the only system that judges whether it is effective through data and behavior mode, as shown in Figure 1 network security evaluation

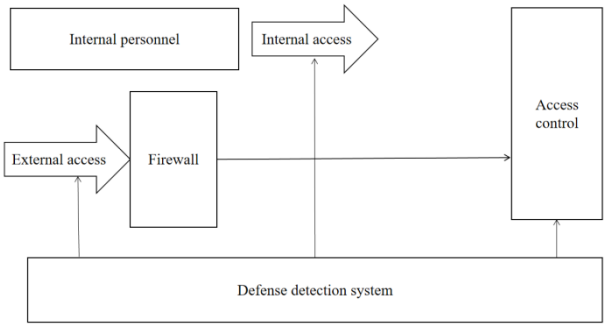

Fig.1 Network Security Evaluation Function of Network Security Evaluation

A firewall is like a door, which can prevent the entry of a class of people, but it can not prevent the saboteurs in the same class of people, nor can it prevent the saboteurs inside. The access control system can prevent people with low-level permissions from doing unauthorized work, but it can not ensure that people with high-level permissions do destructive work, nor can it prevent people with low-level permissions from obtaining high-level permissions through illegal acts. Vulnerability scanning system can find vulnerabilities in the system and network, but it can not scan the system in real time. The network security evaluation system can be classified from different angles, as shown in Figure 2 network security evaluation.

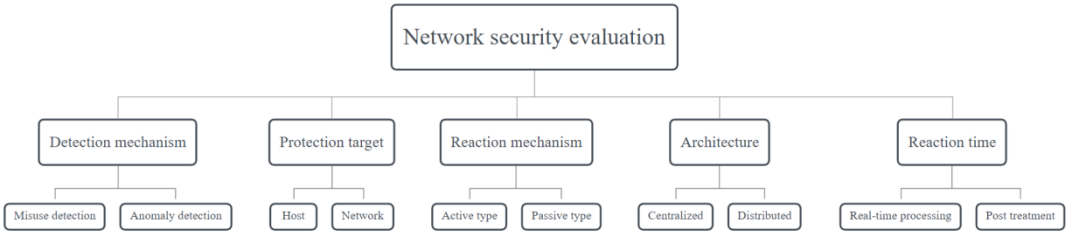

Fig.2 General Model of Intrusion Detection System

According to the different monitoring objects and data sources of network security evaluation system, it can be divided into: network-based network security evaluation system and host based network security evaluation system; According to different detection methods, it can be divided into two categories: misuse detection and anomaly detection.

4. Network Security Defense System Based on Data Mining

4.1 Distributed Collaborative Network Security Evaluation System Based on Data Mining

In order to improve the ability to identify user abnormal behavior and detect unknown attack patterns, this paper proposes a distributed collaborative network security evaluation system framework based on data mining. Its structure includes data collector, conventional network security evaluator, conventional intrusion rule base, conventional security event base, collaborative security event base, collaborative network security evaluator, collaborative intrusion rule base and rule generator based on data mining. By combining misuse detection technology based on expert knowledge base with collaborative network security evaluation, the system has certain ability of conventional network security evaluation and collaborative network security evaluation. Using the association rule algorithm based on data mining, the system can adaptively generate some cooperative intrusion rules with certain support and reliability, so as to have a certain ability to detect unknown pattern cooperative intrusion.

4.2 Unsupervised Anomaly Detection System

Unsupervised anomaly detection method does not need to use any labeled data, which greatly reduces the production requirements of training data set, and has become a research hotspot recently. Clustering algorithm is a typical unsupervised anomaly detection method. This type of method usually assumes that the data set contains a large number of normal data and a relatively small amount of abnormal data, and the abnormal data is essentially different from the normal data. This paper presents a network security evaluation system based on clustering, which can automatically detect new or other unknown forms of attacks. In this system, there is no need to provide manual or other labeled data in the training stage, and it can detect a variety of different types of attacks while maintaining a low false positive rate. The training data set used to establish the model in this method must correctly and fully represent the data distribution of the whole network or host environment. If this premise is not satisfied, the intrusion judgment method used in the system will become unsuitable for the records from a completely different data distribution area or from a cluster that cannot be represented by a known cluster.

5. Conclusions

With the popularization of computer network applications and the increasing frequency of network activities, the problem of computer security has become increasingly prominent. Network security evaluation system is an important part of information security technology. However, the traditional network security evaluation system has deficiencies in effectiveness, adaptability and scalability. Data mining technology is the latest technology introduced into network security evaluation. It can extract the knowledge and laws that people need and unknown in advance from a large number of network data and host log data. Using data mining technology to improve network security evaluation and realize network security is a new attempt.

References

[1] Su Yingying. Network security evaluation and most active defense based on attack defense game model [J]. Network security technology and application, 2017 (4): 2.
[2] Liang Yeyu, Yang Ming, Ning Jianchuang, et al. Research on network security audit technology based on data mining [J]. Guangxi communication technology, 2017 (3): 4.
[3] Li Gen. optimal design of control system based on network security and big data mining technology [J]. Electronic technology and software engineering, 2018, No. 134 (12): 246-247.
[4] Ren Zhen, Hu Xuewen, Zhang Hong. Application of improved FCM algorithm in network intrusion detection [J]. 2021 (2011-5): 42-44.
[5] Liu Ning. Computer network security virus defense based on data mining technology [J]. Computer products and circulation, 2017 (12): 68.
[6] Cai Chang. Research on current situation and defense measures of power network security management [J]. Network security technology and application, 2019, No. 218 (02): 83 + 87.
[7] Zhao fan, Ni Zhimin. Research and application of lightweight Web Intrusion active defense key technology and visual measurement model based on dynamic IP blacklist [J]. China building materials technology, 2018, 027 (001): 70-71.
[8] Zou Weifu, Zhang Yiying, Zhang Suxiang, et al. Research on Trojan virus detection technology based on characteristic behavior analysis [J]. 2021 (2014-11): 105-109.
[9] Li Min, Li Wei, Yu Shi, et al. Research on information security active defense system of power grid enterprises based on big data analysis and unknown threat perception [J]. Science and Technology Plaza, 2016, 000 (008): 82-85.
[10] Du Juan. Application of big data mining technology in network security [J]. Satellite TV and broadband multimedia, 2020, No. 516 (11): 49-50.
[11] Guo Hanke. Discussion on the application of data mining technology in computer network virus defense [J]. China new communications, 2019, 21 (09): 119.
[12] Yu Li. Exploration of computer network virus defense technology based on data mining technology [J]. Modern electronic technology, 2016, 39 (21): 4.
[13] Huang Wei. Design of computer network virus defense system based on data mining technology [J]. Electromechanical information, 2020, No. 629 (23): 146-147.
[14] Zhao Kai, he Wenhai, sun Lili. Computer network security virus defense strategy based on data mining technology [J]. Electronic world, 2018, 000 (023): 53,55.
[15] Du Jingzi, Liu Jiong. Design and implementation of network virus defense system based on data mining technology [J]. Information and computer (theoretical Edition), 2018, No. 400 (06): 60-62.