Design and Implementation of Intrusion Detection System Based on Data Mining Technology

Li Xin

Communication University of China, Beijing, China

Keywords: Data Mining, Network Database, Intrusion, Detection System

Abstract: in Recent Years, Due to the Popularity of the Internet, People's Work, Life Rhythm and Efficiency Have Been Improved, and the Interaction and Sharing of Information Have Been Promoted. However, a Large Number of Computers Are Flooding on the Internet, Which Has Become the Reason Why All Computers in the Huge System Are Attacked by the Internet. At Present, Internet Security is Facing Severe Challenges Such as Hacker Attack, Virus Infection and Online Information Disclosure. in Order to Protect the Computer Network System, Various Security Technology Products Including Intrusion Detection System, Firewall and Identity Authentication Have Been Developed. in Addition, the Real-Time Monitoring of Network Security is Necessary. This Paper Proposes the Data Mining Technology Suitable for Internet Intrusion Detection and Optimizes the Hybrid Detection Model of Network Intrusion Detection System.

1. Introduction

With the Rapid Development of the Internet, Various Fields of Society Are Widely Used. the Number of People Entering the Network and the Amount of Network Information Gradually Increase, Which Greatly Promotes the Circulation and Sharing of Information and Improves People's Daily Business Efficiency. However, Due to the Personalization and Openness of the Network, Every Computer May Become the Target of Network Attack. in Recent Years, Hacker Attacks, Network Fraud and Other Network Incidents Occur Frequently. Especially in Recent Years, the Government Pays More and More Attention to the Information Reform. At the Same Time of Deepening the Reform, It Also Stressed Several Issues Related to National Security and Real Estate Security. That Will Bring Some Degree of Irreparable Economic Loss to the Society [1]. It is Necessary to Increase a Series of Network Information Security Products, Including Network Security Problems, Cooperation of Relevant Departments, Formation of Intrusion Detection System, and Development of Network Information Technology Products and Application Software [2]. At Present, the Research on Internet Detection Technology and System Application is in Progress At Home and Abroad. However, to Improve the Accuracy of Intrusion Detection and Leakage Rate is the Research Goal of Relevant Departments. This is Very Related to the Research of Intrusion Detection Technology in China.

2. Intrusion Detection System Related Technology

The User Behavior of the Network Operating System, and Take Effective Measures Against These Abnormal Behaviors, to Control the Abnormal Situation to a Great Extent.

Invasions, Computers, the Internet and Information Systems, and the Destruction of the Outside World. Its Integrity and Security Are Intruded by External Activities [3]. Today, Testing Means That Special Departments Can Designate Illegal Activities and Use Various Methods to Collect Activities At Home and Abroad. Data and Recognition Behavior Analyze the Overall Activities of the Computer and Identify Abnormal Behaviors [4]. in Order to Identify Data Analysis, and Use Specific Internal and External User Behavior Data Analysis to Be Identified, Real-Time Detection of Abnormal Activity Data Can Be Used for Monitoring Intrusion Detection System. Take Effective Measures for These Abnormal Behaviors to Control Users' Behaviors and Abnormal Conditions [5].

First, during the anomaly detection mode, baseline template technology needs to be used. The

DOI: 10.25236/ISMHI.2019.031

detection of baseline template is within a monitoring range. Moreover, system parameters can be customized. The system also adjusts the parameters according to the actual process such as warning threshold and detection statistics method. A test baseline is used to measure or evaluate a specific characteristic flow. Is it abnormal traffic? Data mining technology developed gradually in the 1980s. Due to the increase of database capacity, especially the utilization of data source of replica warehouse technology can effectively help customers [6]. Make use of the application of information data mining technology. Data mining refers to the extraction of information into patterns, models, rules, concepts, etc. In addition, streaming data transmission technology is also needed. A data flow reference is an information transmission device composed of a series of data packets that can flow in a single direction between a plurality of specified sources and nodes. The content is very accurate and can directly reflect the information between nodes.

3. Requirement Analysis of Inspection System

The design of intrusion detection system is to effectively improve the timeliness of detection, reduce the error alarm rate, optimize the detection model system, and verify through experiments. First, there are three main problems in detecting anomalies. In order to effectively improve these problems, the relevant research institutions will focus on the expert system, using statistical methods to establish some intrusion detection systems for some computer abnormal detection behaviour [7]. Data mining is an application technology based on big data. Intrusion detection is essentially the identification of internal and external systems. Once abnormal activity is found, it is sent to the detector, which is the process of data analysis. In the research process of intrusion detection system, we can make full use of data mining technology [8]. Finally, through the experiment of reducing the false-positive rate of intrusion detection model based on data mining, we can verify the design of the prototype system and apply data mining technology in the intrusion detection system [9]. The rationality of the method and hypothesis is verified by comprehensive test. Intrusion Detection Based on identification marks is to define a series of set rules or identification marks, which can be put into a predefined knowledge base. During detection, the current event is compared with the intrusion mode in the knowledge base. If it is the same, the intrusion is considered to have occurred. Therefore, the IDS based on IDS has high detection rate and low false alarm rate. If the system is not configured correctly, small changes of known attacks may also affect the detection of the analysis. Therefore, the method based on identification marks is an effective solution to detect known attacks, but it fails to detect the change of unknown attacks or known attacks. The advantage of using this method is that it is easy to maintain and update preconfigured rules.

Table 1 Comparison of Intrusion Detection Technologies

Intrusion Detection Technology	Features / advantages	Limitations / challenges
Misuse detection	Intrusion is identified by matching patterns;	New or variant known attacks cannot be detected
Anomaly detection	Using statistical tests of collected behaviors to identify intrusions;	Identifying attacks takes a lot of time
Artificial neural network	Effective classification of unstructured network packets;	It takes a lot of time during the training phase.
Fuzzy logic	For quantitative characteristics	The detection accuracy is lower than that of ANN

According to the functional requirements of intrusion detection system, intrusion detection can collect IP data flow. In the process of collecting important information data, the network flow mechanism provided by the network device is used to realize data collection, improve information collection efficiency and conference network monitoring conditions. Second, the intrusion detection data mining algorithm implements the request. Generally speaking, the past intrusion detection technology, statistics, expert system and other product detection methods, using a variety of levels are shown, the products of each detection system are also very different, network intrusion detection system, mainly scanning the network data, for monitoring the internal network segment [10]. In addition, in order to facilitate the detection of malicious attacks, adjust the ID monitoring. However, the existing intrusion detection system needs relevant personnel to judge through experience.

4. Design and Implementation of Intrusion Detection System

The design of intrusion detection prototype system should follow a principle. The system design technology shall be standardized and follow the standard interface specification. Intrusion detection system can collect network user data and intrusion detection prototype according to the technical specifications of related industries in the design process. The system can meet a certain degree of scalability and operability. Secondly, security should be considered. In the design of intrusion detection system, it is necessary to protect user data from illegal use and ensure the data consistency of network system. Automatic fault check and emergency alarm can be used to remind staff to prevent user data loss or damage. In addition, the intrusion detection system has high recognition accuracy and needs to effectively reduce the false-positive rate. In addition, the application program needs to design a flexible structure, and can continue to design the model based on the hybrid algorithm to improve the accuracy of intrusion detection.

In the design of intrusion detection system, it is necessary to preprocess the recorded data of the system. For example, a decision tree model or a combination of related rules is used to form a decision tree based on association rule set, and parameters are stored to detect system risk. From the function module of IDS, the system based on data mining needs to achieve the design requirements according to different functions. It can be divided into four main functional modules: data preprocessing, data mining algorithm model function, detection module and basic management module. It's a module. Data preprocessing includes two data collection standardization functions. Then, it is the network log data extraction, the standardized use of the extracted data, can not provide the necessary data form for the established model, and the data mining module detection are two offline online discovery methods that can help users to timely process the detection results. Once the intrusion is detected, the system will send an alarm message to the administrator within the time. The basic system management module is mainly used for user rights management and login management. Data management and other functions. From the perspective of intrusion detection system architecture, it can be divided into three layers: user layer, business layer and data layer. Different functional layers have different functional categories. First of all, the user layer mainly provides the interface of intrusion detection system. The business layer is the core of the system. This is the basic function of realizing the core business logic and intrusion detection model algorithm of the system. The data layer stores the detected information for query and processing, plus the hardware platform terminal of the intrusion detection system based on data mining, 1024 M memory, amd 64 and 500 g hard disk. Therefore, the current detection system, network customers and two market clusters of related equipment, can detect.

5. Conclusion

This paper analyzes the data mining technology of deep intrusion detection technology, and expands the technical characteristics. Based on this technology, intrusion detection model based on hybrid model is realized by association rules and decision tree, and system design and function design are explained respectively. This can improve the accuracy of network intrusion detection, reduce the false alarm rate, and provide a reference for the network to optimize the intrusion detection system.

References

[1] Lei Zhang, Jianqing Zhang, Yong Chen. (2018). Hybrid Intrusion Detection Based on Data Mining. 2018 11th International Conference on Intelligent Computation Technology and Automation (ICICTA).

[2] Mohamed Idhammad, Afdel Karim, Mustapha Belouch. (2018). Distributed Intrusion Detection System for Cloud Environments based on Data Mining techniques. Procedia Computer Science, vol. 127, pp. 35-41.

[3] X. Geng, Q. Li, D. Ye,. (2017). Intrusion detection algorithm based on rough weightily averaged one-dependence estimators. Nanjing LI Gong Daxue Xuebao/journal of Nanjing University of Science & Technology, vol. 41, no. 4, pp. 420-427.

[4] Xue Wu, Changxu Wu. (2017). Data Mining on Numeric Error in Computerized Physician Order Entry System Prescriptions. Stud Health Technol Inform, vol. 245, pp. 1386.

[5] Yi Yi Aung, Myat Myat Min. (2017). A collaborative intrusion detection based on K-means and projective adaptive resonance theory. 2017 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD).

[6] Klymash Yulia, Strykhalyuk Bogdan. (2017). Increasing the reliability of distribution systems by the use of intrusion detection system based on ricci flows. 2017 14th International Conference The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM). IEEE.

[7] Asuka Terai, Shingo Abe, Shoya Kojima,. (2017). Cyber-Attack Detection for Industrial Control System Monitoring with Support Vector Machine Based on Communication Profile. 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). IEEE.

[8] Shweta Malhotra, Vikram Bali, K. K. Paliwal. (2017). Genetic programming and K-nearest neighbour classifier based intrusion detection model. 2017 7th International Conference on Cloud Computing, Data Science & Engineering - Confluence (Confluence). IEEE.

[9] Francesco Folino, Gianluigi Folino, Luigi Pontieri. (2017). A Peer-to-Peer Architecture for Detecting Attacks from Network Traffic and Log Data. The 7th International Workshop on Peer-to-Peer Architectures, Networks and Systems (PANS 2017) As part of The International Conference on High Performance Computing & Simulation (HPCS 2017).

[10] Malek Al-Zewairi, Sufyan Almajali, Arafat Awajan. (2017). Experimental Evaluation of a Multi-Layer Feed-Forward Artificial Neural Network Classifier for Network Intrusion Detection System. The 2017 International Conference on New Trends in Computing Sciences. IEEE.