Advances in Engineering Research, volume 150
4th International Conference on Machinery, Materials and Computer (MACMC 2017)

Research on Computer Network Intrusion Detection System

Bo Sun[1, a]

[1] Shandong Labor Vocational and Techncal College, Jinan, Shandong, 250022

[a] email

Keywords: Computer Network, Detection System, Intrusion

Abstract. With the computer virus, hacking and other network information security incidents gradually increase the frequency, people are increasingly aware of the importance of network security. Network security has become the current computer network is facing one of the most important issues. Intrusion detection system as a field of IT information security within the field of a new hot technology, in the protection of network security occupies a pivotal position. This paper introduces the intrusion detection of the content, intrusion detection of the main methods, and based on the computer network security intrusion detection system design.

Introduction

Computer network penetration in people's lives, not only changed the specific way of life of mankind, more importantly, changed the way people access information. It appears to bring great convenience to people at the same time, but also to people's information security has brought a lot of hidden dangers and threats. Once the computer network security problems, is bound to cause information leakage, to bring different levels of economic losses, especially within the enterprise important information, and the situation will be likely to lead to the collapse of the entire computer system. Therefore, in order to avoid the virus and other intrusion into the computer network system, we must take an effective intrusion detection method, design a corresponding intrusion detection system.The anomaly detection method is mainly used to detect abnormal behavior of users and their abnormal use of computer resources. The use of this detection method requires the establishment of the corresponding target system and user activity model in order to pass the model of the system and the user's actual behavior detection, so as to whether the user behavior on the computer network and system to determine the offensive. It has good adaptability and the ability to detect unknown attack mode, but the high false alarm rate, the accuracy of the test results are poor, making its application has been limited [2]. In addition, it is necessary to define the normal characteristics of the computer network and the legal authorization of the user in the system, and to distinguish between the illegal and legal code and the data. It is the main technical difficulty of the current anomaly detection technology.

The hybrid detection method is a comprehensive utilization of both the anomaly detection method and the abuse detection method. Because these two methods have a certain complementary relationship in the practical application process, the organic combination of the two methods can achieve the effect of complement and complement each other, and can improve the performance and efficiency of the whole intrusion detection to a large extent.

The so-called intrusion, refers to all attempts to resource availability, integrity and confidentiality and other acts of harm. It includes both malicious hackers (malicious hackers), including the computer network and the system caused by various acts of harm (computer viruses, Trojans, etc.). And intrusion detection refers to the identification and diagnosis of all intrusion. The specific operation of the computer network and so on a number of key points in the data collection and analysis, through the analysis of the results of the network whether there is an object of attack or breach of network security behavior to judge the signs. Intrusion detection software and hardware used to form an intrusion detection system. It has the ability to safely analyze the collected data and derive useful results and take appropriate protection measures, which is more intelligent than other network security tools.

Intrusion Detection System Workflow

The first step in intrusion detection is information collection, which includes the state and behavior of systems, networks, data and user activities; and the need to collect information at several key points in a computer network system. In addition to the extent possible to expand the detection range of factors, there is an important reason is that from a source of information may not see doubt, but from a few sources of information inconsistency is suspicious behavior or invasion of the most Good logo.

The first two methods are used for real-time intrusion detection, such as pattern matching, statistical analysis and integrity analysis. The first two methods are used for real-time intrusion detection, While the integrity analysis is used for post hoc analysis.

Pattern matching is to compare the collected information with known network intrusion and system misuse of specific templates to detect violations of security policies. In general, an attack mode can be represented by a process or an output. One of the advantages of this approach is that only the relevant data sets are collected, significantly reducing the burden on the system. It is the same way as the virus firewall, the detection accuracy and efficiency are relatively high. However, the weakness of the method is the need to constantly upgrade to deal with the emerging invasion of the way, can not identify the unknown means of invasion. The statistical analysis method first creates a statistical description of the system object, which counts some of the measurement properties for normal use. The average of the measured attributes will be used to compare with the behavior of the network, the system, and any observations are outside the normal range, and the intrusion is considered to occur. The advantage is that it can detect unknown intrusion and more complex intrusion, the disadvantage is false positives, false negative rate, and does not meet the normal changes in the normal behavior of users. Integrity analysis focuses primarily on whether a file or object is changed, usually including the contents and attributes of files and directories, which are particularly effective in discovering applications that are made by Troy. Integrity analysis uses a powerful encryption mechanism - the message digest function can identify changes in the file. The advantage is that regardless of pattern matching methods and statistical analysis methods can find the invasion, as long as a successful attack led to any changes to the file or other objects, it can be found.

In order to facilitate the system administrator to view and analyze the attack information, you need to save the information collected by the intrusion detection system. The stored information also retains digital evidence for the attack. After analyzing the attack information and determining the type of attack, we need to deal with the attack: such as the use of alarm, to the system administrator to send e-mail and other manual intervention to deal with the attack, or use the automatic device directly: Such as disconnecting, filtering the IP address of an attacker, and so on.

Intrusion Detection System needs to Solve the Key Technology

Intrusion detection module collaboration mainly refers to the analysis of data sharing and different detection modules between the complementary or enhanced function, through collaboration can be completed in their work alone can not achieve the function or work objectives. The distributed architecture of the network intrusion detection system detects the heterogeneity of the functional modules of the system and the distribution of the data and detectors in the network so that the inheritance is developed by different developers and has different detection mechanisms and runs in different When the intrusion detection function module or the detection subsystem on the system must consider the data sharing and cooperation between them, it is necessary to provide distributed data acquisition and general data interface to realize the interoperability between different detectors (detectors) , And consider the distributed detector in the distributed intrusion detection system in the organization and the detector detection results of the fusion technology. The sharing of distributed data must also format the collected data to ensure data availability. This mainly involves the cooperation mechanism between the functional modules of the network intrusion detection system and its related technologies: the communication mechanism of the intrusion detection system, the

cooperation mechanism between the functional modules, the data preprocessing and the data fusion technology.

Although each intrusion detection system is conceptually consistent: it consists of a detector, an analyzer, and a user interface. But the specific intrusion detection system in the analysis of data methods, data collection and collection of data types and other key aspects are still very different. The intrusion detection system has a certain level in the analysis of the data source, from the application-based intrusion detection system to the multi-network intrusion detection system, the ability to analyze the data and the scope of monitoring gradually increased, widened; The data of the detection system can be derived from the level of not being higher than its intrusion detection system. That is, the detection results and outputs of the intrusion detection system can be exploited and used for further analysis at levels not less than its intrusion detection system.

The research of the rules of attack rules is to adapt to the changing difficulties and priorities of attack and intrusion. It is necessary to establish a rule knowledge base to meet the development needs of detection technology, so as to improve the ability and effect of detection comprehensively. Intrusion classification rules can be generated automatically by the classification learning program, although the rule extraction process eliminates the manual coding and expert experience components. But there are also the following problems: classification learning requires two prerequisites: a. Have sufficient training data; b. Have determined the analysis of the data used in the characteristics of the property. These two points are particularly important, and intrusion training data is guaranteed to cover all patterns of the intrusion. Otherwise it will not be able to detect some of the "no seen" variants of the intrusion. So, first of all, to determine a measure for the training data set, in order to constantly sum up the training data, when the new training generated when the update. And when the measure is stable, stop the training data collection process. Second, after the audit data is collected, the analysis of those attributes is key to the effectiveness of the analysis efficiency and the effectiveness of the results. In addition, when the collected data is not related to the intrusion activity or can not be used to establish the intrusion detection model, it should not be used as training data. Network events are not independent in terms of timing, so feature attributes should also include temporal statistics between events. These are the key issues and technologies that need to be addressed.

Large - scale distributed intrusion detection. Traditional intrusion detection technology is generally limited to a single host or network framework, obviously can not adapt to large-scale network monitoring, different intrusion detection system can not work together. Therefore, it is necessary to develop large-scale distributed intrusion detection technology. Real - time Intrusion Detection Technology for Broadband High - speed Networks. A large number of high-speed network continues to emerge, a variety of broadband access means endless, how to achieve high-speed network real-time intrusion detection has become a real problem.

Conclusion

In the process of computer network security, the research and design of intrusion detection system is a very important link. A good intrusion detection system can effectively compensate for the shortcomings of the firewall, can provide a reliable guarantee for the security of the computer network, and is a more effective protection technology in the modern network security measures. Although the intrusion detection technology is still in the development stage, but with the community on the computer network intrusion detection system design more and more attention, intrusion detection system application and testing performance will rise to a new level.

References

[1] Yang Degan. Computer network security research [J]. Henan Science and Technology. 2012 (22)

[2] Lan Tianjing. Based on the "cloud" end of the network security research [J]. Information and computer. 2011 (04)

[3] Wang Lei. Computer network security research [J]. Science and Technology Information. 2008 (02)

[4] Lei Ming, Tan Jie. Overview of network security research [J]. Silicon Valley. 2008 (04)

[5] Wang Xiang. Computer security in the process of network security research [J]. Electronic Technology and Software Engineering. 2015 (12)

[6] Liulin. Library Network Security Research [J]. Neijiang Technology. 2012 (02)