Research on Key Technologies of Intrusion Detection Based on Pattern Recognition

Jiao Xue

Xijing University, Xi'an City Shaanxi Province, 710123 Chin**a**

Keywords: Key Technologies, Intrusion Detection, Pattern Recognition

Abstract: With the popularity and rapid development of network and computer technology, countless network users are facing increasingly serious security problems. In computer security and network security, the biggest threat now is network attack and intrusion, as more security protection today. The intrusion detection technology of active defense in technology has become a very important research topic in network security research. Pattern recognition is also a hot topic in the field of computer research. Pattern recognition has achieved good results in clustering and classification of sample data. Clustering algorithms and classification algorithms have many advantages, such as high maturity and speed.

1. Introduction

With the rapid development of the Internet, individuals, enterprises and government departments rely more and more on the network to transmit information. Due to the openness and sharing of the network, it is easily attacked and destroyed by the outside world, and the confidentiality of information security is seriously affected. . The issue of cybersecurity has become a problem that governments, enterprises and the majority of Internet users are most concerned about. Independent mathematics-based computer processing business, document processing and complex intranet, extranet, global Internet development based on simple internal network processing, office automation, enterprise computer processing systems and global Information sharing and business processing within the scope. Information processing capabilities, the system's link capabilities are constantly improving. With the ability to link information and improve the circulation capacity, the security problem based on network links has become increasingly prominent, and hacker attacks have become increasingly rampant, and prevention of deterioration has become a very important issue.

2. The Significance of Intrusion Detection Technology

With the ability to link information and improve the circulation capacity, the security problem based on network links has become increasingly prominent, hacker attacks have become increasingly rampant, and prevention of deterioration has become a very important issue:

According to the survey report of Warroon Research, we can know that almost all of the top 1,000 companies in the world in 1997 were hacked. The 1,000 companies at the top of the world were hacked into hackers almost in 1997.

According to US FBI statistics, the annual loss caused by cybersecurity in the United States is as high as $7.5 billion.

Ernst and Young report that almost 80% of large enterprises suffer huge losses due to the theft or misuse of information security.

In a recent hacker's massive attack, the Yahoo website's network stopped running for 3 hours, which caused it to lose millions of dollars in transactions. According to statistics, during this entire operation, the US economy lost more than $1 billion. With the panic of the industry, Amazon.com, AOL, Yahoo!, eBay’s stock stocks fell, and the technology-focused Nasdaq index (NASDAQ) broke the past. For three consecutive trading days, it hit a new high, rising its potential, falling 63.32. The Dow Jones Industrial Average fell close to 62.50 on Wednesday. Website attacks,

including Yahoo, Amazon, and Buy. Com, MSN. Com, online auction house eBay news website CNN. Com, it is estimated that these attacks slow down 20% of Internet traffic. Our website has been attacked by hackers, but it cannot be compared with the situation in the United States, because our number of users and users are at a very early stage, but the fact is that we cannot but think: at the end of 1993, CAS high energy There is a hacker intrusion phenomenon, the user's permission to upgrade the super privilege. When the system administrator tracks, it is subject to retaliation. In 1994, a 14-year-old child broke into the network center through the Internet in the United States, warning the Chinese Academy of Social Sciences and Tsinghua University system administrators.

Beginning in the late 1970s, computer security research was supported by the US government, including the US Department of Defense (Ministry of Defense) and NIST (National Institute of Standards and Technology) security audits are also being considered in these studies. In 1980, Anderson made another report, this time for the Air Force's customers, using large computers to process large amounts of confidential data. Anderson recommends reporting, reducing the amount of data analyzed, as well as comparing statistical data and overall observation methods, ie, statistical behavior to detect abnormal behavior. When a security violation (statistical) anomaly occurs, it alerts the security officer. Security officials also conducted detailed assessments of the observed data. Anderson's report SRI (Stanford Research Institute) and TRW (American well-known data security company) provide a blueprint for early work. In the mid-1980s, many aspects of intrusion detection technology were deeply influenced by his ideas.

3. Related Research on Intrusion Detection Technology

Traditional security technologies, such as firewalls and encryption technologies, are an important part of the network security protection system, using a "divide and conquer" solution. These techniques implement a static, passive defense that blocks most external attacks, but often does nothing for internal attacks. In network security, only the party that initiated the attack and the protected party have a very clear understanding, and different security measures can be taken for different individuals to achieve targeted. Intrusion detection is a powerful complement to the traditional computer security mechanism, and has become the main direction of the development of dynamic security tools at home and abroad. Intrusion detection (ID) is a security mechanism that dynamically monitors, defends, and defends against system intrusions. Intrusion detection uses proactive defense, which has two key points: proactive and defensive. The intrusion detection system is the second safety gate behind the wall. The core of the intrusion detection system IDS is the intrusion detection technology, which directly determines the intrusion detection capability, the effectiveness and efficiency of the attack detection, and the system's false positives and false negatives.

At present, intrusion detection technology is mainly divided into two types: misuse detection and anomaly detection. Misuse detection is to establish a rule base according to known intrusion means, and the information to be detected is matched with the rules in the library to achieve the detection purpose. The disadvantage is that only known types of intrusion can be detected. Anomaly detection is to detect the user's behavior by constructing a normal user profile. The advantage is that unknown intrusion behavior can be detected. The disadvantage is that the technology is immature and the false alarm rate is high. Intrusion detection methods generally include expert systems, model reasoning, state transition analysis statistical methods, and neural network methods. This paper attempts to combine the pattern recognition and intrusion detection methods in computer graphics, and uses the more mature algorithms in pattern recognition to detect the intrusion behavior. The IDS designed in this paper is a host-based anomaly detection system. The function is to supplement the ability of the firewall to resist intrusion and monitor the security status of the internal network.

4. The Structural Design of IDS

The specific task of the IDS is to first extract various information (such as the number of user login failures) that can reflect the system state and user behavior from the audit of each server at

regular intervals, and normalize the information into the required vector form. These quantized data are then analyzed using an analysis algorithm based on the set of feature vectors that have been established. Finally, respond to the results of the analysis. The IDS includes five functional modules: a data extraction module, an intrusion analysis module, a response processing module, a feature vector set, and a data access module.

The module is at the base of the system is the data collector of the intrusion detection system. Because the IDS is designed as a host-based detection system. Therefore, the data source mainly comes from the system's audit record and the information in the log that can reflect the system running status and user behavior characteristics. But this information is often linguistically descriptive and cannot be used directly for computation and storage, so it is also quantified as digital data. At the same time, these data should be compressed and normalized to meet the requirements of improved detection speed and convenient storage. Finally, it forms the vector form required by the analysis engine.

There are various detection methods in anomaly detection systems, such as statistical methods, neural network-based, and state machine. The IDS uses a method of pattern recognition. This method mainly utilizes the more mature algorithm in pattern recognition technology, and performs fast and accurate vector judgment based on the vector set for the vector that describes the system state and user behavior processed from the data extraction module. In order to complete the purpose of intrusion detection.

This collection is the basis for the analysis engine to make judgments. There are two main types of detection methods: one is to establish a normal user's behavioral profile, and the behavioral alarm (abnormal detection method) that does not occur in this contour has the advantage of detecting unknown intrusion behavior, and disadvantages. The technology is immature and the rate of false positives is high. The other is to establish a feature rule base for abnormal behaviors. The advantage of matching the behaviors in the library is that the accuracy is high. The disadvantage is that only the existing intrusions in the rule base can be detected. This paper hopes to draw on the advantages of both, and at the same time establish two sets of vectors that describe different attributes. One set describes the normal system state and user behavior; the other describes the abnormal system state and user behavior. Use two sets as the basis for judgment to improve the accuracy of the judgment. In addition, the feature vector set should have self-improving functions, such as using artificial intelligence or neural network methods to continuously update and supplement the concentrated vector.

5. Main Body Algorithm Implementation

The purpose of IDS to extract this information is to construct a feature vector that provides current system state and user behavior. Then, the attribute of the feature vector is judged according to the existing feature vector set, thereby knowing whether the system state and the user behavior at this time are normal. The following information is the detection information required by IDS.

•P address, date, time
•The port number
• Number of failed logins
• Flow per unit of time
• Modification of control strategies
• Operation of user information files
• Execution of certain commands (such as cmd, net)
• Access and operation of certain sensitive files (such as logs)
• Establishment of unknown files

GET part of the WWW log

So you can construct such a vector:

In this way, the individual's behavior and system state over a certain period of time can be described by such a vector. For example, a user accesses www via the port address 192.168.4.95. Ciom. Edu. Cn, at this time, the system does not perform sensitive operations such as important

commands and special files being accessed, and the flow per unit time is low. Then, a vector can be used to describe: user vector (192.168.4.95, 02.9 -11:22:05,80, no failed login, low flow per unit time, no control strategy modification, ……) However, in order for the computer to recognize this vector and use the vector for the analysis engine, the vector must be vectored. The digitization of the components representing various feature information, that is, quantization.

In addition, the set of feature vectors that need to be explained is actually stored in the same set of vectors in the two feature vector sets, but the attributes are different. The number of vector set vectors should be large, so the work of building a vector set is also very large, and the composition of the vector set vector has an effect on the detection result. Therefore, the vector set should have the ability to self-modify and improve based on the sample and test results. Based on this, the VC++ language is used for programming. Programs embody the mechanisms and functions of the system. The first thing to do after system startup is initialization. An important task in initialization is to read the vector set into memory. Analytical testing is a core part of the system, including extracting information from various logs, quantifying, and analyzing the information to process the analysis results. In addition, there is a timer that triggers the system to complete a test every other time interval.

6. Conclusion

The network security technology based on pattern recognition has certain characteristics: self-adaptive ability, low cost, high carrying capacity and self-learning ability, etc., to a certain extent, can improve the performance of the security system as a whole. Diversified static analysis and genetic algorithm are effective segments established by the pattern library, which can ensure the rationality and effectiveness of the pattern library. However, the model still has certain defects in practical applications. For example, it is necessary to collect a large number of attack behavior characteristics to ensure the rationality and effectiveness of the pattern library. With the rapid growth of network traffic, the efficiency of the algorithm needs to be further improved. To shorten the reaction time of the system.

References

[1] Wang Yanhua, Ma Zhiqiang. Application and research of Tibetan intrusion detection technology in network security. information Technology. 2009, 6: 41-44.

[2] Xia Wei, Lang Rongling. A review of the research on intelligent detection technology of Dai Guanzhong intrusion detection system. Computer Engineering and Applications, 2001, 24: 32-34.

[3] Reluctant. Implementation of computer security intrusion detection scheme. Computer and Information Technology, 2007, 14: 288, 320.

[4] Gao Xiang, Wang Min. Model of adaptive intrusion detection system based on immune mechanism]. Microelectronics and Computer, 2007, 24(3): 74-77.

[5] Li Shuwen, Sun Min. An intrusion detection method based on immune principle EJ3. computer application. 2006, 12 (26): 68-71.