Application of Intrusion Detection Based on psychology in access control

FU Weinan[1, a], WANG Ziqiao[2]

[1,2] School of Software and Microelectronics,

Northwestern Polytechnical University, Xi'an 710072,China

[a]email: fuweinanawe@163.com

Keywords: Information security; network firewall; data mining; intrusion detection; development trend

Abstract. With the vigorous development of the Internet, more and more people use the network, the computer network to provide convenience, bring benefits, but also make the human face a huge challenge of information security. In the form of the development of modern information technology, a safe network system should not only means of defense, but it is necessary to have a means of firewall, defense, but also be able to real-time monitoring of network security, attack and counter attack, the network intrusion detection system. On the current situation of network security is all kinds of hacker events, network crime, virus has been in the stage of escalating, large portal website, government website, enterprise website, and individual users are these illegal criminals invade object, intrusion types and different, means rich utterly impossible, network security defend without delay. So intrusion detection system came into being. With the development of network intrusion detection technology, so that people have been focusing on the application of data mining in intrusion detection technology, if we can improve the data mining technology into the network intrusion detection, according to the specific characteristics of the intrusion detection system, the basic principle of applying data mining, optimize their combination, this will improve performance of intrusion detection system. This article will use the data mining technology to the network intrusion detection technology in the present situation and the future development trend is discussed.

Introduction

With the rapid development of information technology, the size of the database has been expanded, which has produced a lot of data. To decision makers in order to provide a unified global perspective, people in many areas established a large number of data warehouse. However, these large amounts of data tends to make people unable to discern hidden in which can the decision to provide information support, and the traditional query and reporting tools can not satisfy the full mining the information demand. Therefore need a kind of new data analysis technology in the processing of large amounts of data, and from the extraction of valuable potential knowledge, data mining (DM) technology emerges as the times require, data mining technology is accompanied by the development of data warehouse technology is gradually perfected to[1].

Data mining is a network information technology based on database, artificial intelligence, mathematical statistics and visualization of the four pillars. We know that an algorithm design is divided into three parts: input, output, and processing. The input of the data mining algorithm is the database, the output of the algorithm is to find the knowledge or model, the algorithm of the process is designed to design a specific search method. From three aspects of the input, output and processing of the algorithm, it can be determined that data mining mainly involves three aspects: Mining object, mining task, mining method. Mining objects include some kind of database or data sources, such as relational databases, text database, for object database, history database, multimedia database, spatial database, temporal database, as well as the world wide web (WEB). The mining method can be divided into: machine learning method, statistical method, neural network method and database method. Machine learning can be subdivided into: genetic algorithm, integrated learning, error correcting output coding, clustering analysis, etc.. Statistical methods can be subdivided into: regression analysis, discriminant analysis, etc.. The neural network method can be subdivided into: forward neural network, self-organizing neural network, etc..

Data mining is the non trivial process of automatically extracting the useful information from a large number of data sets, which is the representation of the information in the form of rules, concepts, rules and patterns. It can help decision makers to analyze historical data and current data, and to discover hidden relationships and patterns, and then to predict the future trend of things. The process of data mining is also called knowledge discovery process, which is a very wide range of intersection. Data mining is a new information processing technology and its main characteristics is of database of a large number of data extraction, transformation, analysis and other model processing, and extracting the key data aided decision from. Data mining is a knowledge discovery (KDD) in the process of a particular step, it with a special algorithm from data extraction patterns (patterns). It is not the standard database query language (such as SQL query, but the query content search models are summarized and the inherent law. We all know that the traditional query and report processing is the incident as a result of, and there is no in-depth study of the reasons and the development of things and the rules, and data mining is mainly about the causes of and summed up the law, and with a certain confidence degree to the future forecast, to provide a favorable support for the decision maker's decision.

Current situation of network information security in China

With the rapid development of the Internet, the number of Internet users in China surge. Before 1998, China's Internet Internet users is less than 55 million, now China has already surpassed the United States to become the most populous country in the global Internet, according to China Internet Network Information Center (CNNIC) in January 2013 release data display, 2012 China network popularization rate reached 42.1%, all network population numbers to 5.64 billion, whole year added 50.9 million people. Network has become an important tool for people's lives, economic, cultural and social activities are strongly dependent on the network, the network has become an important social infrastructure. However, the current situation of network and information security is not optimistic.

March 25, 2009, China Internet Network Information Center (CNNIC) released the 2008 China Internet users information network security situation research report. According to the survey, as of the end of 2008, China's Internet penetration rate of 22.6%, more than 21.9% of the global average. Nearly 300 million of the number of Internet users, the total bandwidth of IP, 625G address, the number of mobile Internet users. Inevitably, network security issues are also more rapid. In recent years, with the development of information infrastructure, network security management has become an important factor in the relationship between social stability, especially with the advent of the 3G era, the importance of network security management will be more prominent. Report shows that more than 70% of Internet users are willing to use free internet security software, and nearly 80% of Internet users to provide the security of personal information on the Internet has a different degree of concern, network information security has become an important factor influence the users' online behavior. At the same time, the survey showed[2], 96.1% of Internet users personal computer equipped with information security software, including 70.5% of users choose to use a single brand of safety of packaged software products that contains at least two functions of anti-virus, firewall, security software products. 28% of Internet users use online search service, which nearly 1/3 users also use the online anti-virus services. The above data fully shows the importance of Internet users in our country. It is worth noting that, according to the end of 2008 the number of Internet users in the country, the number of users has not yet installed more than 10 million of the number of Internet users, this data reflects the information security of a large number of Internet users there are hidden dangers. Research results show that 74% of Internet users expressed their willingness to use free antivirus software, which shows that free anti-virus software for the vast majority of Internet users have a greater appeal. Report data show that the current domestic nearly one hundred million Internet users have used online banking professional edition, accounting for 33.4% of the total number of Internet users in china. With the development of China's Internet, Internet users have changed from pure entertainment to shopping, job search, business and other aspects, the demand for network information security is also increasing.

Overview of Intrusion Detection Technology

Invasion is a collection of activities that attempt to harm the integrity, confidentiality, and reliability of a resource. Intrusion detection system is a computer software and hardware system for the detection of the intrusion detection system. Intrusion detection system in user behavior is mainly manifested as the form of data, intrusion detection is illegal hackers attack detection and recognition for the computer system and network system, or the broader sense of the information system, or violations of the security strategy in the event of process. It from the computer system or network collecting data, analysis of data, find suspicious aggression or abnormal behavior events, and to take certain response measures to intercept or attack behavior and reduce the possibility of loss. In the intrusion detection system, the system will the user's current operation generated data with the user's historical operational data according to a certain algorithm were detected to judge the user's current operation is intrusion behavior, take corresponding measures according to the result of the detection[3].

Intrusion detection can be divided into computer host intrusion detection and network intrusion detection according to the intrusion data source. Host based intrusion detection is usually detected in the host's audit log and log files to obtain the main data source, and is supplemented by other information on the host (such as file system attributes, process status, etc.). On the basis of this, the task of detecting the hacker's attack behavior can be detected very accurately. Based on the network intrusion detection is to get the necessary data sources by monitor network data packets, and through protocol analysis, feature matching, statistical analysis and other means to find the hacker attacks, can be real-time monitoring of network data flow, find potential attacks and rapid response. The hybrid distributed intrusion detection system can simultaneously analyze the intrusion detection system from the host system audit log and the network data stream.

Common means of invasion and Prevention

In order to make the intrusion detection system can more accurately and more rapidly report intrusion, designers need to known to all means of intrusion analysis, more accurately describe the essential difference between intrusion packets and normal communication data packets, in order to reduce false positives and false negatives.

Intrusion means is usually associated with the system or protocol vulnerabilities, and when some systems or protocols are eliminated, vulnerabilities are patched, these intrusions will naturally not succeed. The invasion method is also changing, when a new intrusion means is found, or the source code is disclosed, it may cause some kind of intrusion, until people pay enough attention so far.

The attack is roughly divided into several categories, including almost all of the current attack. However, the means of attack show different characteristics over time, new ideas and means of attack is also changing with each passing day, trying to make a perfect classification of the attack is difficult to achieve.

1) detection and network sniffer

An attacker in such an attack in the hope that the network related information. In the target IP address space, scanning or sniffing on it[4].

Scanning technology can reconnaissance to allow connection services and open ports, to find out the distribution of target host port, provide various services and server operating system and some service program version, builds the foundation to the attack. The first thing an attacker must do before the attack is to collect the information of the target network. Network detection is the premise of the attack, most hackers will be before the attack on the target scan. At present, some scanning tools already have more powerful functions, such as NMAP, XScan, Nessus, Retina, and some also have automatic attack function. In order to avoid being aware of the other side of the firewall or IDS, the attacker may also use a slow scan or change the scanning means (distributed scanning).

In spite of this, the scan as a proactive behavior, it is likely to be the victim Cha Jue. The sniffer is relatively more "quiet". Sniffing refers to: in the broadcast network, the attacker can monitor of network, the circulation of all data packets, to get the useful information. Such as Hub connected network, as long as the network card is set to mixed mode can directly receive all packets within the network. With the popularity of the exchange network, the difficulty of monitoring is more and more big. However, in view of the network, the key server or device monitoring once successful, still can get a lot of valuable data. Listening is easy to implement, a lot of listening to the network software also has a powerful function, such as Pro Sniffer. In the hybrid mode of computer is likely to be found, in some cases, to the listeners to send a specific format of ARP packet can be found which card in a listening mode, Antisniff is to use this principle. In addition to the scanning and sniffer, the attacker can also understand the victim network structure through some network utility (Ping, NSLOOKUP, traceroute, whois, finger, etc.), through the search engine queries may contain vulnerabilities w tune site (such as Google hacking).

2) decoding class attack

Through various methods to obtain the password file, and then use the password guessing program to decipher the user account and password. According to statistics, 82% of the network password safe enough, birthdays, telephone, initials, the city abbreviation, English words or their combination is used as an example of the password can be found everywhere, a lot of people in different places using only a password or term does not modify the password. These passwords are hard to withstand dictionary attacks.

Because of the password to crack the tool and dictionary generator can be seen everywhere, to crack the password does not require too much technical knowledge. Similar to the LC5 tool in a short time to get the user name of the Windows system and break the weak password system.

3) unauthorized access attack

By using the system management strategy, the user may obtain the right to operate a higher authority than the legal user. The current operating system is becoming more and more complex, many systems in the release, the default configuration is often hidden loopholes. This will cause a large number of computers to become a hacker's puppet master. For example, Windows2000 can accept the empty password of the user from the remote login, resulting in a large number of users of the system is easily controlled by hackers. Many routing devices on the Internet have also been attacked or leaked too much sensitive information because of the security risk of SNMP protocol.

4) buffer overflow

Buffer overflow when the computer program to buffer zone is filled with data bits exceeds the capacity of the buffer itself, overflow data covering the legitimate data. The attacker with his own carefully designed instruction to cover the legitimate process, as long as these instructions are executed, the attacker has the control of the system. Due to some C language library functions such as strcpy and strcat, gets, sprintf, careless design, many operating systems are inevitably exist such problems. Windows, Linux and UNIX system vulnerabilities and most of the buffer overflow related the troubled global user repeated security issues in recent years[5].

With the security programming has been widely concerned, such attacks will be in the future downward trend. There have been a number of vulnerabilities to explore the model can check out the system's potential buffer vulnerabilities, data execution protection (DEP) technology development has also reduced the risk of buffer overflow. However, due to the C / C++ language used in the operating system is very wide, this kind of attack can not be eliminated in a short time.

Conclusion

With the rapid development of the Internet, the network plays a more and more important role in people's production and life. Enterprises and the country's dependence on the network, but also the number of network security incidents increased year by year. Countries, businesses, schools, individuals are being subjected to a variety of threats from viruses, Trojans, backdoor and hacker intrusion. They may not only affect people's normal life and work, but also may cause property damage. 2003 shock wave and shock wave worm in 2004, leading to hundreds of millions of hosts in the world to restart the countdown to restart, to give people a deep memory. Now, malicious software and network attack means more and more subtle, the average user is barely aware of its existence. At the same time, the objective of network attacks become stronger, because the Internet is difficult to trace, strong concealment characteristics, network crime rate showed a clear upward trend.

Through the Trojan to steal user password, bank accounts, personal data case common occurance, some software for commercial purposes, the client mandatory installation and can not be completely removed, some organizations to attack or damage to the site to coerce, to blackmail blackmail also have occurred. Tens of thousands of the world's control of the botnet has also left a huge network security risks. People's attention to network security, so that the number of network security products and a significant increase in the number of products. Intrusion detection system and intrusion prevention system is one of the hot topics in network security. When the network security event occurs, people hope that the intrusion detection system can timely and accurately alarm, or to take appropriate measures to block attacks. The development of intrusion detection system with independent intellectual property rights has an important role in national security.

Intrusion detection system can be software or hardware. Software has the advantages of good flexibility, but it is difficult to further improve the speed. Modify and improve the existing outstanding open source intrusion detection system, and transplanted it into the open source embedded system, is currently in the hardware implementation of high-speed intrusion detection system, a feasible method. Although its performance compared with the ASIC there is a certain gap, but it is more flexible and easy to achieve.

References

[1] Tang Zhengjun. Introduction to intrusion detection system [M]. Beijing: Mechanical Industry Press, 2004.4.

[2] Liu Wentao. Network security development kit Xiangjie [J]. Beijing: Electronic Industry Press, 2005.10.

[3] Tang Zhengjun. Design and implementation of network data packet analysis tool [J]. Beijing: Publishing House of electronics industry, 2002

[4] Zhang Shibin. Network security technology [M]. Beijing: Tsinghua University press, 2004.8117:160.

[5] W.Richard Stevens[America].TCP/IP Xiangjie volume: [J]. protocol of Fan Jianhua et al. Beijing: Mechanical Industry Press, 2000.4.