

Design and Implementation of Network Security Audit and Monitoring System

Chen Xin

Wuhan Polytechnic, Wuhan, 430074, China

chenxinwuhan@sina.com

Keywords: Network security; security auditing and monitoring; network log; data mining algorithm; log fusion.

Abstract: This paper introduces an example system of network monitoring and auditing based on the technical requirements of network monitoring and security auditing. By sampling and analyzing the network data, the system monitors the behavior of network users, records and alarms the security behavior of the system through log auditing of the host and proxy server, facilitates the publication of network information, and provides the analysis results and statistical data to ADAMI. The administrators have greatly improved the level of network security management and achieved satisfactory results. Firstly, this paper analyses the network security audit log system. According to the need of the design and construction of the network security audit log monitoring system, under the guidance of the design and implementation of the prototype of B/S C/S hybrid system, the architecture of the system is given. Current audit methods generally adopt some methods of analysis and comparison. On this basis, this paper proposes that the system adopts a security audit engine with learning ability, and gives the framework of the security audit engine. Through an example analysis, it proves that the prototype system can achieve real-time monitoring and centralized management. Realize intelligent audit. The implementation of this system can provide strong support for the security audit of network system.

1. Introduction

With the wide application of Internet in the world, the political, military, economic, social and other aspects of the country are more and more cannot be separated from the computer network. However, due to the vulnerability of network security, hacker attacks on the Internet are also growing at what speed. Government, military, post and telecommunications and financial network is the soil to the current attack of hackers. With a variety of network applications become more and more abundant, beautiful and destructive means into the network is more and more advanced, network security technology has become more and more complicated, only by simple means of fire end can't meet the need, need to have more powerful network security system. Due to the variety of means of hacker attacks, effective anti l hacker's entry into the well is not an easy thing to do. In order to computer network security, availability, integrity, the computer network security audit and monitoring is very necessary. Security audit and monitoring technology through real-time monitoring of network activity, analyze the behavior of users and system, audit the system configuration and vulnerability assessment, the integrity of data and sensitive system, identify the attack behavior, the abnormal behavior statistics[1], decoy server record hacker behavior tracking and recognition in violation of safety rules using behavior, and other functions, the system administrator can effective monitoring and evaluation system and its own network. Monitoring and audit technology is an effective supplement to the firewall and intrusion detection system, make up the traditional firewall on the network transmission content of coarse grain (below the transport layer) control, at the same time as an important means of network security, detection means a single intrusion detection system is also useful, timely monitoring of network Specification for the use of network. With the continuous development of information technology, especially network technology faces change rapidly, all kinds of information people for thousands of years has been formed in the transfer mode is being

changed, including a variety of means of communication between people and the corresponding social management organizations is also changing the way. The basic idea is: the general sense of the various data of the network continues to pass the package to collect, and quickly unpack, through analysis of acquisition and reduction to achieve a variety of data corresponding to the upper application protocol, and on this basis, to achieve the use of various specific applications in the implementation of network monitoring, illegal special network to all found to have the ability to implement real-time reporting, when necessary, can also according to the administrator is required to achieve certain host real blockade, effectively cut off its illegal acts on the Internet, so as to realize the network information resources to implement effective management and maintenance[2]. All kinds of security products, technical features, work will also change the corresponding changes, the compatibility of their own problems. So, in order to effectively improve the safety capability of the network system itself, it is necessary to perform some of the selected log audit system separate safety equipment in the system, the respective, thus forming a new security products to achieve a unified security log audit, namely the network security audit system based on log. Are the main features of the system: it is the audit system based on log, and the formation of the network structure, can promptly and effectively evaluate the network security system to establish a variety of security products, especially IDS, firewall, IPPS three security products [3]. The schematic diagram of the security audit and monitoring system is shown in Figure 1.



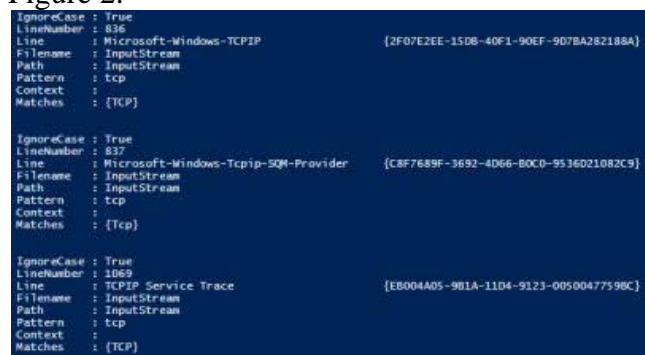
Fig 1. Schematic diagram of network security audit and monitoring system.

The main purpose of this paper is to build log monitoring and security audit platform of a network will be at different locations in the network, the format is not the same kinds of log and audit data unified management, and comprehensive analysis. Its significance lies in: the integration of a variety of security products log information, can effectively avoid the lack of a product such as: it can detect some special attacks cannot be detected by IDS (such as a longer time span long; secondly, the attack) comprehensive treatment, can effectively realize the Intrusion Forensics; finally, through a comprehensive analysis of the comprehensive log data, but also can find some unknown or undetected intrusion etc.. To provide a reliable guarantee for the overall security of an information system. In this paper, the traditional log management, including the basic problems existing in the process of network security audit of these logs in on the discussion, based on the design of a network, network log distributed monitoring and security audit system, and on this basis, the design and implementation of a prototype system, the system mainly take the combination of B/S and the way of C/S. Analysis and Research on the existing security audit log for a variety of products, and on this basis, design a suitable format of the web log conversion "middle log format". In order to solve the problem of different variety of log format fusion; for the design of security audit engine system, through the analysis and comparison of the common safety audit method, mainly have the learning ability of data mining technology to realize [4].

2. Log monitoring and security audit technology analysis

2.1 Web log overview

At present the biggest security products the status quo is the lack of coordination, so many products are piling up, can better guarantee the security of information system. For this purpose, log monitoring and security audit technology has been gradually becoming one of the hot spots to ensure network security, and has attracted the attention of many experts and a variety of different security vendors. At present, the single or single application log monitoring, including on the basis of security audit technology in the domestic and foreign research are more, but also appeared a lot of mature products. But in the face of the network environment, in particular, to achieve a variety of computer systems, monitoring and security audit log, there are still a lot of problems in the technical research. In the current computer system, in order to facilitate the relevant personnel to master the operation of the computer system itself, the general will use some mechanism to describe the computer system itself. The log (LOG) file is one of the most important tools in the computer system. Under normal circumstances, the log file is a computer system, especially one of the important components of the security system. Logs can be recorded in a variety of situations in a computer system (sometimes referred to as audit tracking). The maintenance of a certain information system and the security audit is very valuable. For the definition of log (Log), generally refers to the computer system to specify the specific operation of the object and the results of the operation, in accordance with the formation of an ordered set of time. It is a collection of file systems, relying on the establishment of a variety of data log file. In the computer system, the composition of each log file is realized by a relatively similar method, which is formed by a series of different records. Log files can be distinguished as two parts, namely, the header and the log data segment. Usually, the log files are stored and later maintained by the computer local system that generates the log records. The schematic diagram of the network log is shown in Figure 2.



```
IgnoreCase : True
LineNumber : 836
Line       : Microsoft-Windows-TCP/IP           [2F07E2EE-15DB-40F1-90EF-9D7BA282188A]
Filename   : InputStream
Path       : InputStream
Pattern    : tcp
Context    :
Matches    : {TCP}

IgnoreCase : True
LineNumber : 837
Line       : Microsoft-Windows-Tcpip-SQM-Provider [CBF7689F-3692-4D66-B0C0-9536D21082C9]
Filename   : InputStream
Path       : InputStream
Pattern    : tcp
Context    :
Matches    : {Tcp}

IgnoreCase : True
LineNumber : 1069
Line       : TCP/IP Service Trace              [EB004A05-9B1A-1104-9123-00500477598C]
Filename   : InputStream
Path       : InputStream
Pattern    : tcp
Context    :
Matches    : {TCP}
```

Fig 2. Sketch map of Web log grab.

2.2 Network security audit

International network security audit (network record), is to strengthen and standardize the Internet security, Internet security network and information security, promote the healthy and orderly development, to safeguard national security, social order and public interests. Computer network security audit (Audit) refers to the security strategies, the use of records, system activity and user activity information, environment and activities of inspection, examination and inspection operation events, to find loopholes in the system, the process of intrusion or improve the performance of the system. It is also a process to review and evaluate the system security risk and take the corresponding measures. In the case of non-confusion, referred to as the security audit, the actual record and review the user's computer and network system activities, is an important measure to improve the security of the system. System activities include activities of the operating system and application processes. User activities include activities in the operating system and applications, such as the resources used by the user, the use of time, the implementation of the operation, etc. Security audit review and

estimate independent of system records and activities [6], its main purpose includes 5 aspects: (1) to the deterrent and warning of potential attackers may exist, is the core of risk assessment. (2) the control of the test system, in time to adjust, to ensure that the coordination with the security policy and operating procedures. (3) to assess and provide a basis for effective disaster recovery and accountability for the damage that has occurred. (4) evaluate and feedback the changes in system control, security policies and procedures in order to revise the decision and deployment. (5) to assist the system administrator to find the network system in time to invade or potential system vulnerabilities and hidden dangers. System level audit mainly for system login, user identification number, login attempt the date and time, out of date and time, the use of equipment, operating procedures after login event information review. The typical system level audit log also includes some security independent information, such as system operation, cost accounting and network performance. This type of audit is not unable to track and record the application event, nor does it provide sufficient detail information. The system log is mainly based on the network security level and strength requirements, select the recording part or all of the system operation. If the audit function of startup and shutdown, the use of authentication mechanism, the introduction of subject object address space, delete the object, administrators, security officers, auditors and general operation, and other specially defined audit events. For a single event behavior, usually the system log mainly includes: the date and time of occurrence of the event, the user IP address of the event, the event source and destination location, event type, etc. For a variety of network systems should adopt a different log mechanism. The audit records must include network operation information system, all users in the process and the entity security level at a certain level, including user registration, user registration, super user access, a variety of instruments, other access to state change information, special attention should be paid to the activities of the public on the server or anonymous or guest account other suspicious information [7]. A wide road network security audit system can not only for intranet, Internet behavior management of employees, but also for the network security auditing of Internet behavior. The emergence of the wide channel wireless auditing system enables the network security audit to be covered in the wireless field. The schematic diagram of the network audit is shown in Figure 3.

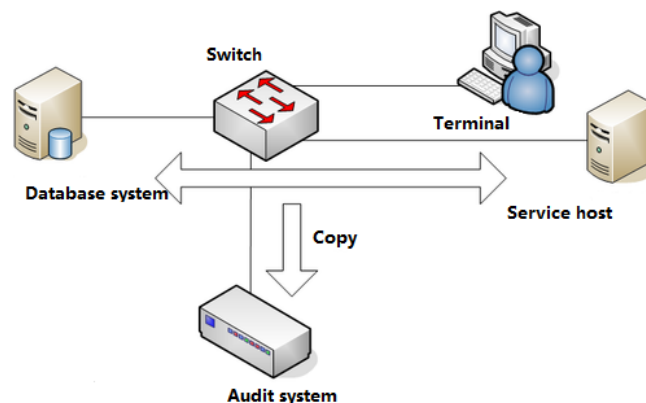


Fig 3. Schematic diagram of network audit system.

2.3 Composition of disaster recovery system

Data mining , also translated as data mining, data mining. It is a database knowledge discovery in one of the steps. Data mining generally refers to the process of searching for information hiding in the data from a large number of data. Data mining is often associated with computer science, statistics, and through online analysis processing, information retrieval, machine learning, expert system (depending on the old rules of thumb) and pattern recognition and many other methods to achieve the above objectives. Need is the mother of invention. In recent years, data mining has attracted great attention of the information industry, the main reason is the existence of a large number of data, can be widely used, and the urgent need to convert these data into useful information and knowledge. Access to information and knowledge can be widely used in a variety of applications, including

business management, production control, market analysis, engineering design and scientific exploration, etc. The use of data mining from the following areas: (1) from the idea of statistical sampling, estimation and hypothesis test (2), artificial intelligence, pattern recognition and machine learning algorithm, modeling technology and learning theory. Data mining has also quickly accepted ideas from other fields, including optimization, evolutionary computation, information theory, signal processing, visualization, and information retrieval[8]. Some other areas also play an important supporting role. In particular, database systems are required to provide efficient storage, indexing, and query processing support. Techniques that are derived from high performance (parallel) computing are often important in dealing with massive data sets. Distributed technology can also help to deal with massive data, and it is more important when the data cannot be concentrated together. Usually, the prediction is played by classification or valuation, that is to say, the model can be used to predict the unknown variables. K-means algorithm is a kind of indirect clustering method based on the similarity measure between samples, which belongs to the non-supervised learning method. This algorithm takes the K as the parameter, divides the N object into k cluster, in order to make the cluster have high similarity, and the similarity between clusters is low. The computation of similarity is based on the average value of an object in a cluster, which is regarded as the center of gravity of the cluster. This algorithm first randomly selects K objects, each of which represents a cluster centroid. For each of the other objects, the distance between the centroid of the cluster and the object is assigned to the most similar cluster [9]. The k-means algorithm is a kind of dynamic clustering algorithm, which is a typical point by point iteration method. The main point is the error square sum as the criterion function. The schematic diagram of K-means algorithm is shown in Figure 4

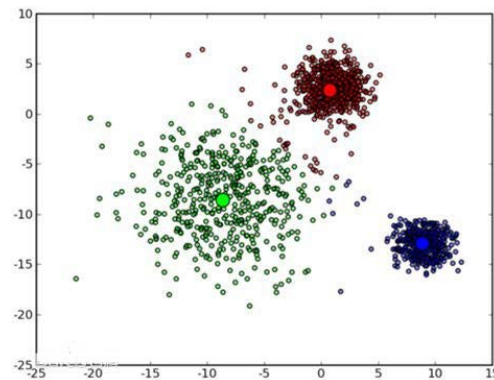


Fig 4 Schematic diagram of K-means algorithm.

2.4 Method of safety audit

The method based on rule base is to extract the corresponding features of the known attacks, and then describe the features and put them into the specified rule base. Under normal circumstances, this method has a special effect on the use of specific hacking tools for the implementation of the attack. However, the security audit method based on rule base has its own limitations. This method is difficult to meet the requirements of the system for those very easy to change, or potential, as well as the rule base does not have the characteristics of the attack behavior. Safety audit method based on mathematical statistics, we need to detect object generates a statistic description, such as: the average value and variance of network traffic, according to network, the first statistical values selected in the normal circumstances, then the value of practical data in the network the package into and out of the corresponding, if found the actual value and the normal value detected large from imitation, generally can be considered there is a potential attack. But the limitation is that how to correctly determine the normal values and non-normal numerical threshold is a problem in the actual situation, the administrator is generally depends on the experience, this situation will inevitably lead to some false positives and false negatives. This section mainly analyzes the technology of log monitoring and security audit. Mainly introduces basic situation of logs, mainly the development of monitoring and management technology of log situation, and main trend of its development, at the same time for

some of the current major security audit methods are analyzed and explained. So as to lay a theoretical foundation for the next step [10].

3. Log monitoring and security audit system requirements analysis

3.1 Log acquisition requirements in a network environment

Distributed in the network system in a number of devices under normal circumstances will produce the corresponding log to their various acts or related to a variety of network events recorded. But the reality is that, due to the inconsistency of the manufacturer, the log of different equipment or system is different, mainly in grammar and semantics. If you want to build a log of all the equipment for the security monitoring and auditing, so as to form a centralized platform, in the key problems which need to solve is the first, at different locations in the network, and how a log format can effectively collect. In the network environment, due to the diversity of network nodes, the diversity of equipment, it will inevitably bring the diversity of the log. In the face of these various kinds of log, this paper will be divided into four main types: operating system log, security equipment log, network equipment log, application system log. Especially in some confusion situation, these four kinds of log in this paper take the "Web log" manner as. The so-called system log, in general terms, mainly refers to the NT/2000 Windows and other operating systems in various components in the operation of the various events to record the data. In these records of events generally can be divided into: the major problems in the system driver in a variety of operating system components; major problems appeared in the operation; and the applications in the operation of the major issues and these issues mainly include the important data loss and error. But for the domestic, the current more popular commercial intrusion detection system log format but with the Snort log format is relatively close, despite this, or to achieve a certain degree of compatibility. In addition, the current mainstream of the commercial level of security devices generally provide a text file to download the function of the log file, or these devices are also available to take syslog protocol to achieve the function of log file transfer[11].

3.2 Network equipment log

Network equipment log is mainly refers to the network to achieve the network connection of the device itself generated by the log, these devices, including switches, routers, etc. For various types of high-end switches and routers generally will take a certain way to record the running state of the equipment itself, and the system in the operation of some of the more unusual record. In addition, in terms of compatibility, the network equipment usually provides for Syslog RFC3164 (The BSD syslog Protocol) support various log processing mechanism and the agreement clearly provides support, therefore, transmitted through syslog protocol to realize various equipment between multiple logs. The so-called application of the system is to refer to the work process in the system, mainly by the application, or system of some important events generated by the different procedures, and to record the formation of the log. For example, in the database, the corresponding program is completely possible to achieve a certain error in the file recorded in the application log. In general, events that are required to be recorded are determined by the developer according to the needs of the user. It is also worth noting that the archive (or offline) log is a system option, which can be configured for selection. In addition, once an Oracle database instance of the online log data will be full of the situation, the archive operation, so as to form the necessary files. In order to facilitate the identification, will be archived online log files for unique identification, and the same logo to merge to form an archive log. This requires that all kinds of log format must be familiar with the format; otherwise the corresponding log to deal with the time there will be some difficulty. In addition, there is a considerable part of the log (such as Windows) and will not take the text way to record the log information, in this case, must use special tools to analyze these logs.

3.3 Security audit requirement

Data mining technology is developed with the development of database technology. Because of the continuous application of database and its management system, it is urgent to understand the important information which is hidden behind the data. Therefore, it is hoped that the higher level analysis of the existing data, to achieve a better use of these data. Under this demand, and gradually formed the realization of data storage in database management system, analysis of the data has been stored to realize a machine learning method, which can extract the useful knowledge behind the large number of data, the effective combination of the two forms of knowledge discovery in database .

3.4 Design and implementation of log monitoring and security audit system

Two key issues must be solved for the acquisition and audit of the network log records. One is how to collect the different logs, but to establish the comprehensive analysis and security audit of the network log data. In order to obtain the log, design a kind of intermediate log format to carry on the mutual transformation, unify the format. In order to construct a reasonable and effective security audit engine, this paper uses data mining technology with learning ability The basic idea: Based on historical log data collection enough on using a classification algorithm to generate a classifier to realize and judge the new log data audit, from the analysis of what normal behavior is, and which is suspicious behavior, which is intrusion behavior.

4. Summary and Prospect

The log for the management of computer systems, especially the security of the computer, has very important significance, therefore, various studies on log monitoring and security audit technology has been a hot research topic. In this paper, we design a real time monitoring and centralized management, as well as the main function of the intelligent audit network log monitoring and security audit system prototype. And the corresponding research and implementation are carried out with the prototype system as the main line. Based on the various products of the existing security audit log in-depth analysis and research, design a suitable for the web log conversion "log format", so as to solve a variety of network environment in the fusion of different log; through the analysis and introduction of the safety audit method, in when constructing the security audit engine, taken with the learning ability of data mining technology to realize, and gives the framework of security audit engine; the design and implementation of a specific network log monitoring and security audit system. Through the example analysis, the analysis results show that: through data mining, so as to achieve the concentration, the collected log data statistics, correlation, clustering and other operations, can be analyzed conveniently from the large amount of log data and extract the corresponding security information, this information is difficult to achieve in the traditional security audit mode this, intelligent audit logs to a certain extent.

Acknowledgment

Funded by Hubei Province Education and Science Planning Annual Key issue in 2016"“The Study on Relationship between Enterprise Education and Entrepreneurial Quality in Higher Vocational Colleges“, (NO:2016GA060).

References

- [1] Xie Yan, Zhang Guoge, Yu Wei, Jing Jie. A preliminary discussion on the information security of the network within the trusted control [J]. Information security and technology. 2015 (02).
- [2] Wu Shizhong. Highly concerned about the information security of the ten major systemic risk [J]. China information security. 2014 (01).
- [3] Ma Zhaofeng, Kong Dan, Jiang Ming. Design and implementation of security audit system based

on cloud platform [J]. Information security and communication security. 2013 (10).

[4] Chen Jianchang. Network security analysis under the big data environment [J]. China new communications. 2013 (17).

[5] Zhang Jian, Chen Jianfeng, Wang Qiang. Research on cloud computing security audit services [J]. Information security and communication security. 2013 (06).

[6] Zhang Guangxing, Qiu Feng, Xie Gang, Tong Hongxia. An efficient network flow record indicates that the method of research and development of [J]. Computer. 2013 (04).

[7] Sun Yongjie. The government and enterprises should parallel information security standards in China need to line [J]. Communication world and Europe and the United States. 2012 (46).

[8] Wu Minmin. [J]. information security technology and the necessity and technical construction of enterprise computer network security audit system. 2011 (Z1).

[9] Zhou Ruiling, Ye Jin, Xie J. association rules data mining methods for the improvement and implementation of [J]. Small and microcomputer systems. 2002 (03).

[10] Pan. Research on Data Mining Based on association rules [J]. Journal of Zaozhuang teachers' College (05) (2001).

[11] Huang Jin, Li JB. [J]. intrusion detection firewall log information based on computer engineering. 2001 (09).