Research and Evaluation of Security Audit Technology in the Era of Network Security Level Protection 2.0

Zhijie Li and Hui Suo
School of information engineering, Guangdong mechanical & electrical college, Mali village, Zhongluotan town, Baiyun District, Guangzhou City, Guangdong Province, China.
Email: 5294968@qq.com

Abstract. With the release of network security level protection 2.0 standard, the work of equal protection evaluation is facing unprecedented challenges. How to deal with it? This paper takes the security audit technology as an example, starting from the concept of network security audit technology, analyzes the security audit object, combines the security audit evaluation index to evaluate the network security equipment, operating system and database system, and puts forward the prospect of security audit evaluation according to the problems in the evaluation practice.

1. Introduction
On May 13, 2019, the equal protection 2.0 standard was officially released, and it was announced that the series of standards would be implemented on December 1, 2019. The network security level protection 2.0 standard changed from passive protection to active protection, and from static protection to dynamic protection. The level protection 2.0 standard refers to the security audit requirements in the evaluation system of security area boundary, security computing environment and security management center. The security area boundary audit mainly refers to the important security events and user behaviors of network and equipment; Security computing environment audit mainly refers to user behavior, security events, subject object access behavior, etc.; Management Center audit mainly refers to various operation logs of administrators. Security audit is not only to meet the needs, but also the focus of enterprises. This paper analyzes the security audit of network security equipment, operating system, database system and other business systems based on the security audit evaluation index.

2. Security Audit Evaluation Object
2.1. Network Security Audit Technology
Audit has a very long history in China. Zafu in the Western Zhou Dynasty, Bi Bu in the Tang Dynasty, the audit institute of the Republic of China and the Audit Office of the people's Republic of China are all specialized audit departments. Their purpose is to check whether the behavior of people and the allocation of resources meet the requirements of the norms. If they violate the corresponding laws or norms, they will leave relevant evidence. There is also a special audit department in the financial system to collect and analyze the evidence of the unit's data, so as to assess the financial situation of the enterprise and make relevant conclusions and reports.

The security audit in level 2.0 standard is the same as the traditional audit concept, which is compliance inspection. Through data analysis, it checks whether the user behavior, process behavior,
communication behavior, system operation, etc. meet the requirements of relevant specifications; All of them are independent. Audit role, audit account number, audit work, audit equipment and audit system are all operated independently; The audit process is the same as the collection, sorting and analysis of audit evidence. The content of information security audit is changed into digital evidence, i.e. log, event, message, etc.; the audit function is still supervision, appraisal and evaluation, real-time monitoring of system operation status and human operation behavior, providing data evidence, analyzing and judging system and user compliance, and providing audit reports.

2.2. Analysis of Safety Audit Objects
With the rapid development of information technology, the information system is becoming more and more complex. The evaluation requirements of level protection 2.0 are more stringent. Which objects should be audited? Next, the audit objects are analyzed from the host, network, database, operation and maintenance, log, business and configuration.

The host audit is mainly based on desktop management, which audits and manages the logs and user operation behaviors of windows, Linux and other servers or clients, including illegal access control based on network or host, terminal operation audit, mobile storage media management, etc. The content of terminal operation audit is more complex, including file creation, saving, modification, deletion and replication, network access based on application layer protocols such as HTTP, SMTP, FTP, IP address and MAC binding, printing and other user operations.

The integration of network audit and intrusion detection is high, including network behavior audit and network security audit. Network behavior audit is mainly based on the management of HTTP, SMTP, FTP and other network protocols. The same is true for ordinary enterprises and public security systems. Network security audit can be managed from two aspects: network intrusion detection and advanced sustainability threat detection.

Database audit mainly covers the audit of MySQL, Oracle, MS SQL server, infomix and other database system operation behaviors. It needs to conduct security audit on the security vulnerabilities, system configuration, abnormal operation behaviors, etc. in the database.

The security operation and maintenance of the system also needs to be audited, including identity authentication, operation authorization, behavior audit, account management, single sign on and other audit functions.

Various log information in the network system can be accepted through syslog, SNMP Trap, FTP/SFTP, Agent, APM, etc, Overview the security status and operation status of all network devices. For example, the security log information of network devices, security devices and operating system can be collected through syslog.

Security audit is required for OA, ERP, financial software, payment software and other specific businesses of enterprises, and for middleware business systems such as IIS, Apache, Weblogic, etc.

In the security audit system, improper configuration of software and patch, hardware and operating system will bring great loopholes to the security of the system. Configuration audit is very important. Configuration audit system or change inspection system can make configuration audit easier.

3. Security Audit Evaluation Practice

3.1. Evaluation Index Division
The network security level protection standardizes the security audit from three aspects: security area boundary, security computing environment and security management center. It requires to ensure the availability, integrity and confidentiality of audit logs from audit scope, audit strategy, log record, log storage, audit analysis, audit protection, etc.

The boundary of security area includes four evaluation indexes. One is to audit the security of network boundary and important network nodes. The audit covers every user and audits important user behaviors and important security events; The second is that the audit record should include the date and time of the event, the user, the event type, whether the event is successful or not and other information related to the audit; The third is to protect audit records, make regular backups, and avoid the expected deletion, modification or coverage; the fourth is to be able to conduct independent
behavior audit and data analysis on user behaviors of remote access and Internet access. Security computing environment includes four indicators. One is to enable the security audit function, which covers every user and audits important user behaviors and important security events; The second is that the audit record should include the date and time of the event, the user, the event type, whether the event is successful or not and other information related to the audit; The third is to protect audit records and make regular backups to avoid the expected deletion, modification or coverage; The fourth is to protect the audit process and make regular backups to avoid unexpected deletion, overwriting or modification. The security management center includes two evaluation indexes: one is to identify the audit administrator; the other is to allow the audit administrator to conduct security audit operations through specific commands or operation interfaces, and audit these operations; The second is to analyze the audit records through the audit administrator, and deal with them according to the analysis results, including storing, managing and querying the audit records according to the security audit strategy.

3.2. Audit of Network Security Equipment
Because of the business characteristics, switches and routers can only identify and record the network information and fault records, and cannot match all the security audit evaluation indicators in the level protection 2.0 evaluation system. The traffic analysis log device can effectively make up for these, and support the analysis of user behavior, network status, etc. In Huawei or H3C routing switching and other network equipment, start the logging service by the command "Info Center enable", "Info Center + subcommand or parameter" can be used to set the network interface, information storage location, information security level, etc. Each information includes eight levels: debugging, informational, notifications, warnings, errors, critical, alerts, and emergencies. The next generation firewall has powerful functions, integrates some functions of log flow control, and is more powerful than switch routing equipment in log control and management.

3.3. Operating System Security Audit
In Linux, error log and audit log are used to audit the security of the system, while in windows, audit policy is used to audit the security of the system. The error logging in Linux system is completed by syslogd and the daemons of all kinds of application systems (FTP, samba, etc.), the system kernel calls syslog to add error information to / var / log / messages. The audit log system in Linux provides a way to record system security information. When users violate the rules of security behavior, it provides warning information, which is composed of audit, audit and other programs. Audit receives audit information from the kernel through the netlink mechanism, writes the audit information to the audit log file, and distributes it to the background process dispatcher to call syslog to write to the system log. Linux security audit mechanism also needs to be flexibly used to reach the evaluation standard of level protection 2.0, such as history log, which records a large number of user operation commands, but does not establish security audit rules for it, which cannot be used as log directly, so it must be implemented in combination with specific scenarios and assisted by other audit tools; for example, SFTP service, there is no SFTP log in the system, so it needs to be communicated Through the configuration of / etc / SSH / sshd_config file to achieve effective audit upload and download file operations.

3.4. Database System Security Audit
The database security audit system monitors and records all kinds of operation behaviors of the database server, analyzes the network data, analyzes all kinds of database server operation behaviors in real time, records them in the audit database, and can query, analyze and filter in the future, so as to realize the monitoring and audit of the database system user operation. By setting different application rules according to different scenarios, we can judge the behavior of illegal operation database and record and alarm it. The traditional database security audit mainly depends on the log files in the database system, and there are many disadvantages, such as the audit function of the database itself will lead to the reduction of the database performance, the existence of various security vulnerabilities in the database product itself, the database administrator can operate the audit log files at will, and the
audit strategy formulation also has randomness. In order to accurately monitor the database activities, it is very important to use a professional database audit platform. The database security system and log audit system are effectively isolated. The audit is to monitor and record all kinds of operation behaviors of the database server for each SQL command of the database, and multiple devices work together to complete the database security audit.

4. Problems and Prospects of Security Audit Evaluation
Network security level protection 2.0 puts forward high requirements for system security audit. Traditional security audit methods can not meet the new security audit requirements, especially the audit strategy which completely depends on network equipment, operating system and database system itself will be impacted unprecedentedly. To carry out reliable security audit on network system, it is necessary to systematically formulate audit strategy Thirdly, adopt specialized audit system.

5. References
[1] Shaoliang Chen 2019 Design of network security vulnerability scanning system based on deep learning in the equal guarantee 2.0 era China Computer & Communication vol 13 (China: School of Humanities and information, Changchun University of Technology) P 86
[2] Xuran Lin 2019 Analysis and preliminary practice of technical requirements of grade protection 2.0 standard Network security technology and Application vol 10 (China: Institute of computer application in nuclear industry) P 14
[3] Shuling Yin 2019 Development and application of information security audit technology Digital communication world vol 9 (China: Hubei Vocational College of science and technology) P 166
[4] Jianyong Fan 2019 Research on the application of database security audit system in Colleges and Universities China new communication vol 21 (China:Shaanxi Normal University) p 43
[5] ChenDing 2019 The practice of big data and artificial intelligence technology in bank network security risk management China Informatization vol 5 (China: Beijing World Star Technology Co., Ltd) p 68