ATLANTIS PRESS

Advances in Computer Science Research, volume 70

2nd International Conference on Mechatronics Engineering and Information Technology (ICMEIT 2017)

The Research on MySQL Security Baseline

Yanhui Ma

School of Computer Science and Technology, Harbin Institute of Technology, Weihai, China

18363122135@163.commail

Keywords: MySQL, database security, security baseline, minimum security guarantee.

Abstract. At present, information system has been widely applied to various fields, but different kinds of database leaks and other security incidents continue to appear, leading to endless security risks for users. Database as the core of information system, the research on which seem to be very important. In order to improve the security of database, setting up security baseline of database properly brooks no delay. The security baseline of database system is the basic guarantee to ensure the safety of the database system. This paper studies the key attributes of database security and their role in database security, and on the basis, this paper gives the MySQL database security baseline, which provides the basic evidence for the security configuration of MySQL.

1. Introduction

Along with the rapid development of information system application technology, database application has gone deep into the national economy, people's production and life, as well as other fields, becoming an indispensable part of social life today. So the security of the information is becoming more and more important and companies tend to pay more attention to its integrity, availability and confidentiality. In most cases, the information will be stored in the database, while the security of the database itself, which is responsible for the storage and maintenance of data, is facing unprecedented challenges. Any damage to the database may result in extremely serious consequences. Therefore, how to make the database system more secure has become the focus point people research on and concern on.

2. The security and threats of database

2.1 The security of database

Now there is no uniform definition of the concept of database security at home and abroad. At abroad, the definition of database security is most widely affected and accepted [1] by C.P.Pflagger, who describes the database security from the aspects of the integrity of the physical database, the integrity of the logical database, the security of the elements, the accessibility, the access control, the authentication and the usability. In China, the database security [2] is to ensure the confidentiality, integrity, consistency and availability of the database information, among which confidentiality refers to protect the data in the database from leaking and unauthorized access. Integrity means to protect the data in the database not to be destroyed and removed; consistency is to ensure that the data in the database satisfies entity integrity, referential integrity and user's defined integrity requirements; availability refers to ensure the data in the database not available to authorized users for human or natural reasons. The security technical requirements of database management system includes identification, marking and access control, data integrity and database security audit.

2.2 The threats of database

At the moment, the main threat to the database comes from two aspects: hardware and software [3]. The threat of hardware is mainly due to some special reasons, such as disk damage, system crash and so on, which can be solved by local or remote database backup. The threat of software mainly comes from the SQL injection, virus infection, human error, password loss and so on. Among them, the SQL injection means the loopholes in the program because of the negligence of programmers. Thus,

someone may login without account and gains the authority of the database operation, so as to steal the database information and even tamper with the database content. In order to reduce the threat of SQL injection and improve the security of database, programmers are advised to pre-compile SQL statements and bind variables. The threat of virus infection can be reduced through the use of anti-virus software, such as Kingsoft anti-virus, 360 anti-virus software and so on. These anti-virus software can find the virus of the existing system, then clean up to maintain the database security. Not qualified configuration to database by database administrators generally lead to the threats of human error, password loss and so on. Therefore, a reasonable configuration of database can significantly reduce the human error and reduce the threat to the database.

3. Database Security Baseline

Database system security baseline [4] means that the related attributes involved in database security should be made necessary and reasonable arrangement in the process of database configuration, which is the minimum security guarantee and the most basic security requirements. It is necessary to balance the cost and the risk to ensure the security of database, and the security baseline is just the reasonable boundary. Therefore, the construction of database security baseline has become the first step to ensure the database security, which is also a prerequisite to solve the problem of database security.

Database security baseline mainly includes five types [5], namely physical security baseline, database patch baseline, database configuration baseline, database health baseline and database business baseline. The first one means the physical protection of equipment and data resources. The second one is the most basic configuration requirement of the account, password, authority, log and so on for the database administrator. The third one means that the database must meet the requirement of the patch. The fourth is the indicator of whether or not to meet the requirements in the running state for the database. The last one means baseline-learning on the current business information of the database.

In this paper, we consider the database configuration baseline and the patch baseline to improve the security of the database. Database requires user authentication strictly. Every user must use the only account and corresponding password for authentication, so as to facilitate the subsequent audit trail. Besides, according to each account's different right to database, a user account could only access the authorized system resources, with no permission to other sensitive information protected by other users, which will help the database administrator to restrict the access of users to particular database. Log and audit can monitor and record of all kinds of database operation, and restore them to audit database, which is convenient to query and analysis in the future. Moreover, it will also benefit to tracking the illegal operation of the database and subsequent database recovery operations. To check and update database regularly, install security evaluated patches and upgrade instantly, and refresh the virus and malicious code library constantly can effectively prevent system from attacks of viruses, Trojans, phishing, web software and other malicious software. At present, enterprises commonly use databases such as Oracle database, SQL Server, DB2, MySQL and so on. Based on the MySQL database, we do a research on MySQL database security baseline, with reference to literature [6, 7] about related configuration parameters and command.

4. MySQL Security Baseline Configuration

4.1 Account Security

In order to improve the security of the database to reduce the threat of external threats, it is the first to increase the protection of the entrance of the database. The user account and password is equivalent to the door key to the database, and the higher security level of the key is more security of the database. The database administrator assigns different user accounts to log on different databases and restrict the user's rights to improve the security of the database.

Account Management Security Baseline Requirements

The database administrator should delete or lock the account that has nothing to do with the database operation, maintenance and so on. In order to meet this condition, the database administrator

first need to obtain all of the users' information from the user table. The following command could be executed.

mysql>select * from user;

This command show all information of users to the administrator. If there are independent accounts, database administrator may use drop command to delete them.

4.2 Password Security

If there is a default user in the database using the default password, this will reduce the security of the database. Therefore, database administrator need to modify the default account password, otherwise the attacker may use the default account and the default password to intrusion database and threat the system security. In order to reduce the occurrence of such a situation, the database administrator can enforce the complexity of the password, such as length, duration, case and so on.

Account Password Security Baseline Requirements

The database administrator should check whether the account uses a default password and a weak password, depending on that the length of the password is at least 8 bits and the password includes numbers, lowercase characters, uppercase characters and special characters. The password should include at least two types of the four type. If there is a weak password, administrator need to modify it. The following commands can do this operation.

mysql>update user set password=password ("Hello123") where user='ma';

mysql>flush privileges;

At the same time, the password should be required not to set the same within 5 times and the password should be replaced at the most 90 day.

Authority Allocation Policy Security Baseline Requirements

The database administrator should allocate the minimum rights required to the user according to the business needs of the database. In order to meet this condition, the following command may be used.

mysql>select * from user;

mysql>removke * ;

The first command is used to gain all rights of all users. After this, database administrator could determine whether there is unnecessary or dangerous authorization. If it exists, using the REVOKE command to recovery.

4.3 Log Audit

The log can record the users' operations to the database, including login account, whether login is successful, the operation time and the corresponding operations such as add, delete, change, check, so as to be convenient to query the day after. Therefore, it is necessary to open the database log function.

Log Configuration Database Baseline Requirements

The log function should be set for the database. MySQL mainly includes five kinds of log, respectively, the error log, the query log, the slow query log, the update log and the binary log. In the MySQL command line, the following command may do works.

mysql>show variables like "log%";

This command could be used to display all the types of the log and the status of the logs. Generally, MySQL must be opened the error log. As for other log functions, database administrator need to use command to open them.

4.4 Other Configurations

Patch Security Baseline Requirements

The database administrator should ensure that the database system has installed the latest security patches. In order to meet the conditions, database administrator can view the current database version using the command: mysql –v. After compared with the safety of the latest version, if it is the latest version does not need to update, otherwise update to the latest version in the premise of business and network security. Also it should be through compatibility testing.

Remote Access Security Baseline Requirements

If the network connection is forbidden, it can prevent password attack, overflow attack and sniffing attack. However, it can only be applied to the condition which the application and the database on the

same host. The database administrator can modify the MySQL configuration file /etc/mysql/my.cnf to allow remote connections.

Instead of skip-networking the default is now to listen only on

local host which is more compatible and is not less secure

bind-address = 127.0.0.1

Now MySQL is allowed remote login. If database administrator delete the # before the bind-address, the MySQL will not be allowed remote connection. Database administrator determine whether the need to open this feature according to the different application scenarios. For example, if there is a need to deploy the application scenario, administrator should to open the remote access function.

Access Policy Security Baseline Requirements

Database should only be accessed by the trusted IP address. To achieve this goal, the following command may be used.

mysql>grant all privileges on db.* to username@'IP/netmask';

After this operation, the database can only be accessed through the trusted IP address.

Connection Number Security Baseline Requirements

The database administrator should set the maximum number of connections based on machine performance and business requirements. In order to set this condition, the database administrator can modify the option of max_connections in the MySQL configuration file /etc/mysql/my.cnf. After modified the option, is will work to restart MySQL service.

5. MySQL Database Security Baseline Score

In accordance with the previous description of the database security baseline detection, we have detected the MySQL database and then, we have used the way of weighted accumulation to evaluate the results. According to the importance of the database security baseline detections, we made a floating interval. And according to its importance to fluctuate, the higher the degree of importance, the higher the weight is. For example, the default password and weak password for database security are relatively important, so the weight will be higher. However the important degree of the alert log and update log is relatively low, so the weight is low. Once the standard is established, the database can be scored, and the score is higher, the degree of database security is higher. Here the range of the score is from 0 to 9 according to the importance. And detected result will be 1 or 0. If the result is 1, it means the database is consistent with the database baseline in this item. If the result is 0, it means the database is not consistent with the database baseline in this item. The detected results of MySQL are in table 1.

Table 1. The detected results of MySQL database security baseline.

num	item	Weight	result	score
1	Administrator prohibition	7	1	7
2	Useless acount	2	0	0
3	Default password	7	1	7
4	Weak password	6	1	6
6	User's policy	5	0	0
7	Error log	3	1	3
8	Warning log	2	0	0
9	Slow query log	2	1	2
10	Update log	2	0	0
11	Binary log	2	0	0
12	Latest patch	4	1	4
13	Remote access	2	0	0
14	Trusted IP address control	6	0	0
15	Connections	5	0	0
Database Conformity		52.7%		
Detected total scores/total scores		29/55		

Table 1 shows the detected results of the MySQL database security baseline. Every item of the security baseline was detected. The result for every item is 1 or 0. The score of every item is the multiplication of weights and result. For example, the database has been configured the item of the error log, so the result is 1 and the score is 3. However because the database has useless accounts, the result is 0 and the score is 0. The detected total scores of the database is the sum of the individual score and the database conformity is equal to the detected total scores / total scores *100%. The database conformity can clearly show the security degree of the database. The higher conformity of the database, the security of database is higher. Otherwise there is a need to reconfigure the database to improve the security of the database. Using this detection method and evaluation method, the database administrator will have a good reference and scoring standards.

6. Conclusion

In order to make every item of the database baseline reasonable, database administrator must refer to the relevant standard requirements, which not only can effectively reduce the risk of database system, greatly reduce the cost of the security system and improve the security of the database, but also provide a good reference for the database management for the database administrator and reduce the possibility of error for human.

References

[1] Pfleeger C P, Pfleeger S L. Security in Computing. 3rd Editon. NJ: Prentice Hall, 2003.
[2] Jiao Yan. With Regard to the Status of the Database System Security Research. Network &Computer Security. 2010(5):45-47.
[3] Hu Xiaomin. Computer network database security threats and Countermeasures [J]. China New Telecommunication. 2015(13):98-99.
[4] Liu Tong. Study on the securiy baseline of complex information system [J]. Chinese Journal of Management Science. 2000(s1):636-644.
[5] Ma Xianhu, Xu Li, Jin Huasong. Security Protection Strategy of Database Based on Baseline Technology [J]. Computer & Telecommunication. 2013(4):28-31.
[6] Widenius M, Axmark D P. Mysql Reference Manual [J]. Dec 2009 - World Bank, Washington, 2002(4).
[7] Seidman C, Smith P. MySQL: The Complete Reference [M]. McGraw-Hill, Inc. 2009.