Importance of Security in Database

Hamed Pourzargham

OWDT, LLC , Houston, Texas, United States

Abstract
Database servers are one of the servers that face the highest risk of attackers according to a Forrester study .The sensitive nature of these systems arises from the fact that these servers store the critical assets of o organizations among them details about clients , financial records among other assets making the need for database security even more essential . This paper highlights the main risks that database face and the possible solutions that can be used to mitigate them. Database specific attacks among them excess privileges, and general system vulnerabilities are discussed . The discussion concludes by discussing two measures that can be used to reduce the attacks on databases.

Keywords:
Database, Security, Excessive Rights, Denial of Service Access Control.

Introduction

Just like the other assets that need protection from the users, the valuable and sensitive data that is stored in computers databases are some of the assets that need uttermost protection .In this regard the best safety measures are an imperative aspect of any database beginning from the inception to the design stages. As such, modern techniques need to be implemented to ensure the security of the databases that ensure security, protection, as well as proper defenses at different levels among them the physical , host data and host applications [1].

In the most basic sense, a database can be defined as the collection of data and information that is related in which the facts of the information have an implicit meaning. For example, social security numbers, the name and the birthdays of the users are examples of facts that can be stored in the database. Essentially, databases are created for the purpose of storing data that is logically interrelated and represents a certain aspect of the world [3]. The information has to be collected, processes and accessed to the users .In addition the databases are made according to a specified data model that is used for defining the manner in which the information as well as the relationship between them can be represented .It is noteworthy that the group of programs that offer the various functions of gathering maintaining and data access is referred to the database management system (DBMS) [1].

Maintaining database security is a complex process that needs accuracy and professionalism.. The higher the complexity of the database the more complex the measures that are needed to ensure optimized security .Various networking aspects and connections to the internet can further complicate the security issues of databases [3].Furthermore, the additional users that are added to the base can develop more security concerns . The purpose of this ISI paper is to give an evaluation of the main techniques and facets of database attacks and the security measures needed by focusing on the specific issue of data inference.

Database-Specific Attacks

Excessive Rights

This type of attack takes place when either the users or the applications are issued privileges that are in excess of the requirements of their functions. The main risks if that the rights can be used illegally to access classified data [3]. For instance, an administrator at work whose task needs only read only rights can take advantage of the excess rights to change the salaries of employees. The solution to the excessive rights aside from implementing the appropriate policies for employees is access control through query level . This technique restricts the rights to the least required data as well as operations. The bigger percentage of the traditional security platforms provide some of the functions among them RLS [2] . However m the manual aspect of the tools fail to make them practical as far as limited deployment is concerned.

System Vulnerabilities

Threats and vulnerabilities in the operating systems can result in unauthorized access of data as well as file corruption. This was witnessed when the Blaster worm wet past the vulnerabilities in Windows 2000 to bring down the servers that had been targeted [2] .IPS equipment can be the best techniques of identifying and blocking the attackers that are created for explaining the platform vulnerabilities.

Manuscript received May 5, 2015
Manuscript revised May 20, 2015

Denial of Service

This can be provoked by various ways among them buffer overflows , corruption of data , the flowing of networks and heavy consumption of the resources available .Resource consumption is a unique DoS that stems from the general environment of the database . Preventing DoS can take place at the different layers like the network and the applications. Some of the recommendations to addressing the DoS include the deployment of IPS as well as the rate controls [2] .By opening numerous connections , the controls can ensures that the individual users do not consume the server resource.

Insufficient Authentication.

Systems that have insufficient processes of authentication give room to the malicious attackers to take the identity of being legal users of the database. Some of the attack techniques used include social engineering and force attacks [4]. The use of passwords or two-step verification is needed to reduce such attacks. To make it easier to use , the authentication procedures should be used with the infrastructures of users .

Security Measures

Authentication

This is the initial phase of gaining access to the database . Most systems have various methods through which the users can authenticate the dataset . these methods hold a significant amount of risk especially in the case where proper authentication is not exercised . Some of the threats include passwords and the default accounts [4] . One of the measures that can be implemented to address these threats include locking the database accounts followed by creating the passwords that are related with the default accounts such that they expire once they are installed [3]. This means that only a few accounts will be accessible once they are installed . It is essential that before the users start using the system , the default credentials are modified. In most systems , this can be done by performing the following command :

dba_users_with-defpwd
The command above enables the administrators to check the accounts that have default passwords. This can be done by placing the following query
SQL> SELECT *FROM (insert the command above)
Although the operation eliminates default accounts, it is not possible t verify all the passwords through the view above mainly because some are specific to applications and the database systems cannot be made aware of the accounts that are applications specific [4] .In this regard, it is important for the administrators to carry out a check that verifies all the default accounts and eliminates them . This can be done by account listing.

Access Controls

The exercise of verifying the access controls is an imperative aspect of securing databases. After users have gained authentication, the controls can be sued to decide what each use is allowed and restricted to do. Historically, some usability issues have contributed to the granting of users excess privileges than they required posing serious threats to the systems. When assigning the access controls, it is important that the privileges of each user are analyzed as well as the privileges that are assigned to the PUBLIC [3]. The query below can be used to view the privileges assigned:
SQL > SELECT * FROM dba_sys_privs.
Separating the roles is similarly imperative and can be applied variously in different environments [4].For instance the tasks of the administrator and auditor should not be the same as each one has its own access needs. The separation of environments is also imperative ranging from production, testing and development . Since links act as the pathways that escalate the user privileges, then they need to be reviewed constantly to make sure that only the links that have been authorized are leveraged [4]. It is also essential to make sure that all the links are stored in the same environment. The administrators should carry out an analysis of each link and its purpose so as to reduce escalation.

CONCLUSION

As has been seen in this discussion database security is essential to protect sensitive information that can be used negatively by malicious persons . Since databases are quite complex , database administrators need to be aware of the security impacts of the wide range of configuration options that they have .For instance by focusing on the aspect of availability , DBAs can easily overlook the configuration concerns that might potentially create vulnerabilities in terms of security issues and compromise private data .The applications as well as access and encryption pose risk to the databases especially in the back end . With this in mind it is important that the security measures that have been highlighted above be executed correctly to reduce the risk of attacks on databases .

References:

[1] Tendick, P., & Matloff, N. (2012). A modified random perturbation method for database security. ACM Transactions on Database Systems, 47-63.
[2] Shaul, J., & Ingram, A. (2007). Practical Oracle security your unauthorized guide to relationial database security. Rockland, Mass.: Syngress Pub.
[3] Basta, A., & Zgola, M. (2012). Database security. Boston, Mass.: Course Technology/Cengage Learning.
[4] Natan, R. (2005). Implementing database security and auditing a guide for DBAs, information security administrators and auditors. Burlington, MA: Elsevier Digital Press.