International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 6 512 - 513

Database Security: A Study on Threats & Attacks

[1]ganesh Shankar Pote, [2]prof. Anandhi Giri
[1]MCA Student, YMT College of Management
[1]ganeshidp@gmail.com
[2]Professor, YMT College of Management
[2]*giri_anandhi@hotmail.com*

Abstract-A paper focuses on a study of the Database Security which becomes a major issue in the present era. In the Today's Environment of fastly increasing need of" Database Security" from Threats & Attacks. The following paper gives a brief information about some concepts about Database Security and also discuss the issues like Threats and Attacks.

Keywords-*Database Security, Threats, Attacks*

*****

INTRODUCTION-

Introduction or data is one of the most valuable asset in any organization. Every organization whether social, governmental, educational etc. have now computerized their Information system. They have maintained the databases which contain delicate information. Database security is serious measure to protect confidential data which can be stored in the database. Database Security deals with generate database secure from any kind of illegal access or threat at any level. Organizations that are running successfully have challenge to maintainPrivacy of their database. They doesnot allow the unknown user to access their data/Information. And they are also having challenge to assurance that their data is protected against Infectious modification. Data protection and confidentiality are the major security concerns.

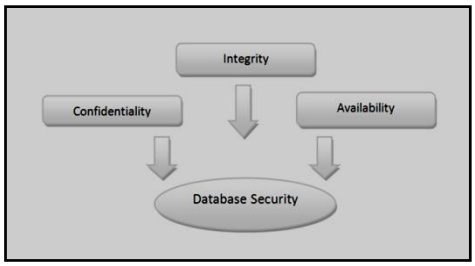

Fig 1 Properties of Database Security [1]

In the today's world security is important and challenging task that people are facing all over the world. Security in e-market world having great demand. Actually database security means protect the sensitive data stored in a database [4].Following are different security layers in a database which are database admin security officer, system admin, developers and employee [4] and security can be added at any of these layers by an attacker.

CATEGORIES OF ATTACKER -

An attacker can be classified into following classes [5]:

INTRUDER -

An Intruder is an anonymous person who has no authority to accessing a computer system in an illegal manner and try to get some delicate information which is stored in database.

INSIDER -

An insider is not authorize person but a member of group of trusted users and makes violet authorize person privileges and tries to get information beyond user's own access permissions.

ADMINISTRATOR -

An administrator is an authorized person who has full control over a computer system, but he/she uses his/her administration privileges in illegal way. According to organization's privacypolicy to spy on DBMS behaviour and to get valuable information.

DIFFERENTTYPESOF ATTACKS -

After violating through all the layer of security, any one of the two following attacks can be carried out by an attacker [6]

DIRECT ATTACKS -

Direct Attack is attack which is carried out by direct hitting. These attacks are successful only if the database doesnot accommodate any security system. If this attack fails, the attacker moves to the next attack.

INDIRECT ATTACKS -

Indirect attack which is not directly executed on the target but data from or about the target can be collected through other intermediate object. to cheat the security system, some combinations of different queries are used. These types of attacks are difficult to track.

Attacks on database can be further classified into two types [6]:

PASSIVE ATTACK -

It monitors unencrypted traffic and looks for clear-text passwords and vital information that can be used in another types of attacks. Passive attacks can include traffic analysis,it monitors unprotected communications and capturing authentication using passwords. Passive attacks results in the display of information to an attacker without the knowledge of the user.

ACTIVE ATTACK -

In specified attack, the attacker tries to break the secured systems. Attack can be done through stealth, viruses, worms, Trojan horses etc. It willtry to break protection features, to introduce malicious code and to steal information. These attacks are mounted against a network backbone,it exploit information in transitand electronically

attack anlegal remote user during an attempt to connect to an enclave. Active attacks result in the display of data files, DoS, changes in data.

THREATS TO SECURITY IN DATABASE -

EXCESSIVE PRIVILEGE ABUSE -

When database users are granted enormous allowance,it exceeds required job function, than these privileges may be abused for malicious purpose. E.g. a user in a company have the rights to modify employee contact information may take advantage of excessive database update privileges to change salary information. [8]

LEGITIMATE PRIVILEGE ABUSE -

It occurs when anlegal user mistreats their legitimate database privileges for illegal purposes. Legitimate privilege abuse comes in existence when the database administrators misused their rights and doing any unconstitutional or unethical activity [8].

PRIVILEGE ELEVATION -

Sometimes errors are detected in software then attackers can take it as a chance to convert their access rights from normal user to those of an administrator, which could result in fake accounts, funds transfer, and misunderstanding of certain analytical information [8].

PLATFORM VULNERABILITIES -

Vulnerabilities in operating systems such as window XP etc. and additional services installed on a database server may lead to illegal access. E.g., the Blaster Worm is a type of computer worm which spread on Windows 2000 vulnerability to construct denial of service conditions [8].

DATABASE SECURITY CONSIDERATION -

To remove the security threats every organization must consists a security policy which should be implemented to secure data. A strong security policy must contain well defined privacy features.

ACCESS CONTROL -

It maintains communication between databases.In other system objects are as per the policies and controls defined by organization. No tampering generated by any attacker neither internally nor externally and thus secure the databases from potential errors. Errors can be critical which can create problem in firm's operation. Through controlling access rights may also useful in reducing the risks that may precisely impact the security of the database on the main servers. For instance, if any table is deleted accidently the results can be roll backed for specific files, but through applying the access control their deletion can restrict.

INFERENCE POLICY -

It is important to protect the data at specific level. It occurs when the analysis of particular data in the form of facts are required to gain a certain higher security level. It also helps to determines how to protect the data from being released.

USER IDENTIFICATION /AUTHENTICATION:

This is the very basic way to ensure security since the identification process generate a set of people who are getting authority to access data. To maintain security, the identity is authenticated and it keeps the delicate data secure and from being modified by anonymous user.

ACCOUNTABILITY AND AUDITING -

These are used to ensure physical integrity of the data.It requires defined to get access to database and it can handled through auditing and for keeping the records. The data placed on servers for authentication, accounting and access of a person can be analysed with the help of auditing and accountability.

ENCRYPTION -

Encryption is the process in which information is converted into a ciphertext so that it can be readable to people those who hold a key for the cipher text. The cipher text is called as encrypted data.

CONCLUSION-

For any organization data is most important property. Protection of sensitive data is always a challenging task for an organization at any stage. Databases are easy target for attackers because of the information it contains. it can be accommodated in several ways. Different types of attacks and threats are available today from which a database should be protected. It prevents the sensitive data from attacker which considerations we have to adopt is mentioned in this paper.

REFERENCES –

[1] Sweety R. Lodha, Web Database Security Techniques, International Journal of Advance Research in Computer Science and Management Studies, Volume 2, Issue 3, March 2014,Page(s):300-305.

[2] Kadhem, H.; Amagasa, T.;Kitagawa, H.; A Novel Framework for Database Security based on Mixed Cryptography; Internet and Web Applications and Services, 2009. ICIW '09. Fourth International Conference on; Publication Year: 2009, Page(s): 163 –170

[3] Luc Bouganim; Yanli GUO; Database Encryption; Encyclopedia of Cryptography and Security, S. Jajodia and H. vanTilborg (Ed.) 2009, page(s): 1-9

[4] International Journal of Computer Science & Emerging Technologies (E-ISSN: 2044-6004) 368 Volume 2, Issue 3, June 2011, page(s); 368-372.

[5] IqraBasharat, FarooqueAzam, Abdul WahabMuzaffar,"Database Security and Encryption: A Survey Study", International Journal of Computer Applications (0975 – 888) Volume 47– No.12, June 2012.

[6] Emil Burtescu, "DATABASE SECURITY - ATTACKS AND CONTROL METHODS", Journal of Applied Quantitative Methods, Vol. 4, no. 4, Winter 2009

[7] Mr. Saurabh Kulkarni, Dr.SiddhalingUrolagin, "Review of Attacks on Databases and Database Security Techniques", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 2, Issue 11, November 2012.

[8] Deepika, NitashaSoni,International Journal of Advanced Research in Computer Science and Software Engineering, Database Security: Threats and Security Techniques,Volume 5, Issue 5, June 2015, page(s); 621-624.