Mara International Journal of Scientific & Research Publications
Vol. 1, No. 1, September 2017, Pages 40 - 48

Understanding Database Security Metrics: *A Review*

Jane Juma* and Daniel Makupi
School of Computer Science and Bioinformatics
Department of Information Technology Security
Kabarak University, Private Bag 20157, Kabarak, Kenya
Email: jjumacloy67@gmail.com

* Corresponding author

Received: August 1, 2017
Published: September 4, 2017

Abstract

The ever increasing demand for high software reliability requires more robust techniques for software quality and security level prediction. Databases are the core of Information Systems (IS), it is therefore necessary to ensure that the quality of the databases in order to ensure the quality of the IS. Recently, it has been a challenge to determine on what is a good database model or design. Therefore, in our discussion we have considered measuring specific features and factors in a particular database implementation. The variant features and characteristics inherent to a particular database serve to come up with a metric of assessment.

Keywords: Database Metric, Assesment, database, database security

1. INTRODUCTION

Databases are the repositories of the most important and expensive mission critical information in the enterprise. Today, in many business organizations, the databases and data assets are poorly protected from external attackers as well as insiders. Databases must be secured well as any other systems in the organization. They allow data to be retained and shared electronically and the amount of data contained in these systems continues to grow at an exponential rate. So, the need to ensure the integrity of the data and secure the data from unintended access has emerged, (Cavoukian and Jonas, 2012). To secure a database environment, many database security models are developed. With the increase in usage of databases, the frequency of attacks against those databases has also increased. Database attacks are an increasing trend these days. What is the reason behind database attacks? One reason is the increase in access to data stored in databases. When the data is being accessed by many people, the chance of data theft also increases (Al-Sayid and Aldlaeen, 2013). In the past, database attacks were widespread, but were less in number as hackers hacked the network more to show it was possible to hack and not to sell proprietary information. Another reason for database attacks is to gain money selling sensitive information, which includes credit card numbers, Social Security Numbers (SSN) among others. In order to have a proper discussion and understanding of database security metrics, we first need to define database security metric as a standard of measurement that enables quantification of the degree of safety of a database. It measures how likely a database system is to suffer damage from attack. A database metrics helps:

i) To evaluate performance and protection of the database.
ii) Monitor database security in a proactive measure.
iii) Contribute to the improvement of the existing database security practices

iv) Help management monitor database security

v) Justify database related security budgets

1.1 Statement of the research problem

The security assessment of a database application over time has proved to be difficult to implement. The assessment in place is per usage, at the user level understanding but not measurable. Therefore, this method has been occasioned with a non-deterministic conceptualization of how secure a design and a model of a database should be. Therefore, our discussion will serve to inform on inherent factors that can be used as a metric of assessment.

1.2 Objective of the study

Our main focus is to come up with a framework that would aid banking institutions to measure the security status of their online banking infrastructure by commutatively considering banking facilities, investments and defense in-depth strategies (SSOB).The status will serve to appropriately inform the security posture of the banking institution.

2. SURVEY OF LITERATURE

Database technologies are a core component of many computing systems. They allow data to be retained and shared electronically and the amount of data contained in these systems continues to grow at an exponential rate. So does the need to insure the integrity of the data and secure the data from unintended access. The Privacy Rights Clearing House reports that more than 345 million customer records have been lost or stolen since 2005 when they began tracking data breach incidents, and the Ponemon Institute reports that the average cost of a data breach has risen to $202 per customer record, (Razdan and Bommakanty, 2001).In August 2009, criminal indictments were handed down in the United States to three perpetrators accused of carrying out the single largest data security breach recorded to date. These hackers allegedly stole over 130 million in credit and debit card numbers by exploiting well-known database vulnerability, an SQL injection (Murray, 2010). The Verizon Business Risk Team, that has been reporting data breach statistics since 2004, examined 90 breaches during the 2008 calendar year. They reported that more than 285 million records had been compromised, a number exceeding the combined total from all prior years of study (Murray, 2010). Their findings provide insight into who commits these acts and how they occur. Consistently, they have found that most data breaches originate from external sources, with 75% of the incidents coming from outside the organization as compared to 20% coming from inside. They also reported that 91% of the compromised records were linked to organized criminal groups. Further, they note that the majority of breaches result from hacking and malware often facilitated by errors committed by the victim, for instance, the database owner. Unauthorized access and SQL injection were found to be the two most common forms of hacking, an interesting finding given that both of these exploits are well known and often preventable. Given the increasing number of beaches to database systems, there is a corresponding need to increase awareness of how to properly protect and monitor database systems.

At its core, database security strives to ensure that only authenticated users perform authorized activities at authorized times. It includes the system, processes, and procedures that protect a database from unintended activity. The Defense Information Systems Agency of the US Department of Defense (2004), in its *Database Security Technical Implementation Guide*, states that database security should provide controlled protected access to the database content and, in the process, preserve the integrity, consistency, and overall quality of your data (Murray, 2010). The objective is simple, the path to achieving the goal, a bit more complex. Traditionally database security focused on user authentication and managing user privileges to database objects (Guimaraes, 2006). This has proven to be inadequate given the growing number of

successful database hacking incidents and the increase in the number of organizations reporting loss of sensitive data. A more comprehensive view of database security is needed, and it is becoming imperative for students in the computing disciplines to develop an understanding of the issues and challenges related to database security and to identify possible solutions.

3. DATABASE METRIC FACTORS

Database security should always be SMART to be counted as being effective. The security metrics should indicate the extent to which the goals set are being met and be driven towards organization overall aim of information security. With changing needs of information and database security in organizations, there is no denying that good metrics take care of the need to secure database systems while observing the security principles. Organizations employ a number of different metrics and a combination of them to make their databases secure. Operational effectiveness and demonstration of strategic value comes to effect when those responsible for information security function try to scrutinize their information systems.

3.1 Database security metrics factors

There are three fundamental factors that governs database security, these are:

i) ***Foundational defenses and coverage*:** these are data securing factors which strive to provision confidentiality, authentication and availability of information. They should be taken into consideration and these entail anti-virus, anti-spyware, firewalls in use etc.

ii) ***Patch latency*:** is the time from when a patch is released to the time it is deployed. Patch latency helps identify business units with outdated or missing patches and which might raise the need for central patch management or improvement of the process.

iii) ***Authentication*:** passwords use and strengths should also be taken into account. The passwords should be with password-complexity and harder to crack and any weak spots in the systems should be addressed. Attacking password is very easy through use of password cracking programs. These attacks could target desktops, admin systems and servers. The time required to break a password of your systems should be considered, for instance, is it prone to cracking during lunch hour when admin is not on his desk? Like in this scenario (Fig. 1) example a case of MySQL database vis-à-vis Oracle database. The security architecture in the two databases is that the way MySQL is implemented is prone to Security breaches compared to Oracle. The following diagrams below shows the demonstration;

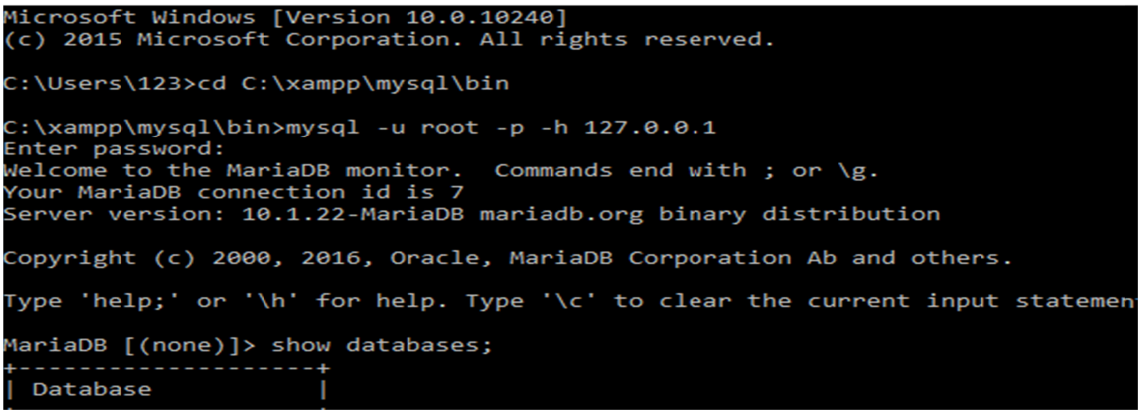


Fig 1: Login authentication for MySQL (Researcher, 2017)

From Fig. 1 sample above, it can be clearly seen that access to the database does not need strict use of password. A user can easily access the system at any privilege level especially given the fact that MySQL does not enforce strict rules for passwords to authenticate users.

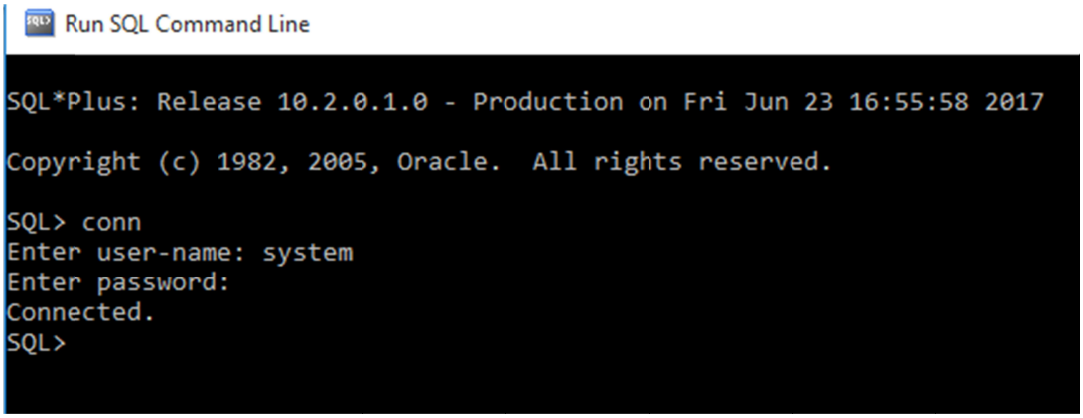


Fig. 2: Login authentication in Oracle (Research data, 2017)

In Fig. 2 example above, in case of Oracle base, a user has to provide a username to start with, and is set per user level privilege. Once the user enters the correct username it prompts entry of password. The user has to enter matching password to the level as shown above which actually enforces security.

Implementation process: *MySQL* is such that it does not force a user on strict authentication mechanism during installation; as such it does not require strong password authentication practices. Oracle, on the other hand forces a user to use strong password combinations during installation. It further requires a password before the user is logged into the system.

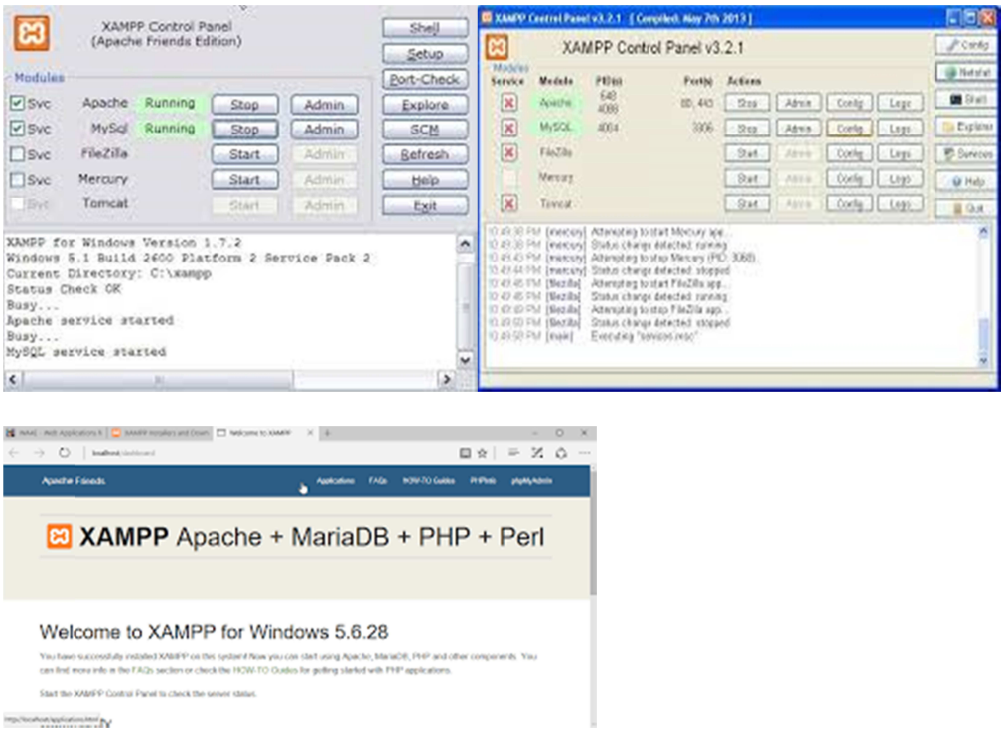


Fig. 3: Screenshots of MySQL installation process (Research data, 2017)

It can be noted that during installation of MySQL it does not enforce strick rules on passoword requiremnet and also combinations.

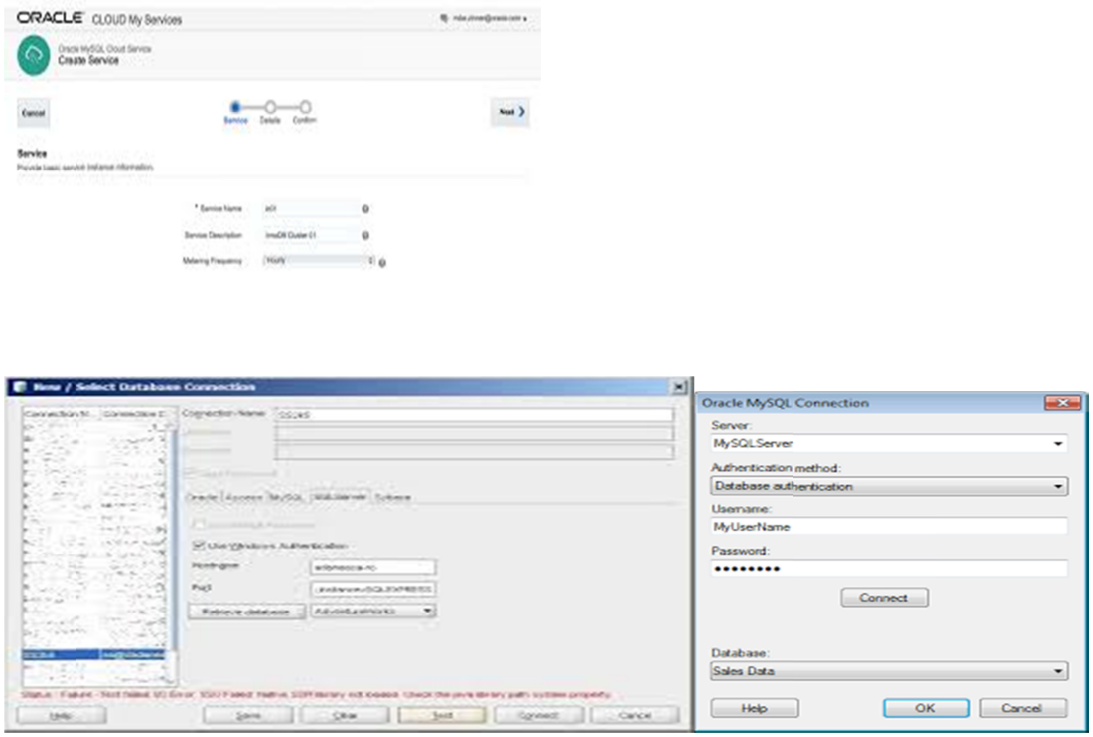


Fig 4: Screenshots of Oracle installation process (Research data, 2017)

From Fig. 4 above, it can be seen that Oracle enforces a password strict requirement that ensures that during installation a strong password combination is used.

***Running compliance and standard scores*:** Organizations adhere to certain best practice guidelines to ensure that information security lapses are not overlooked. These scores endeavor to see that only a few points of access are available, ports are not left unnecessarily open. An illustrative example is shown in Figure 5 below regarding user level privilege and revoke.

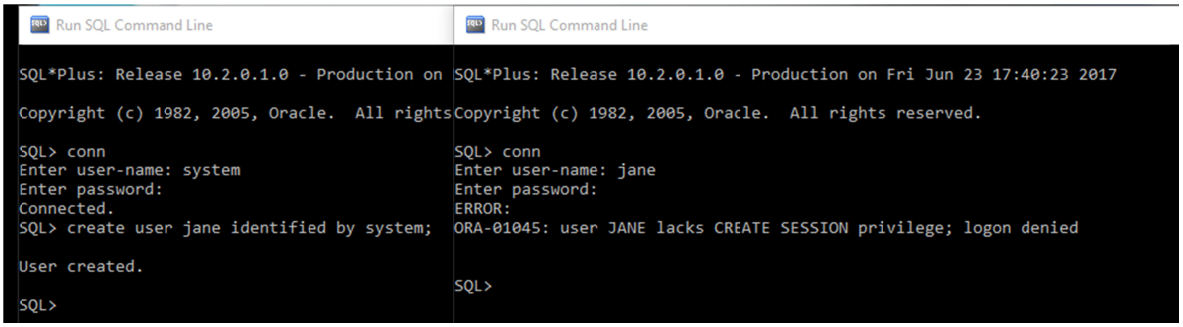


Fig. 5: User privilege levels (Research data, 2017)

From the above Fig. 5, it can be noted that from a user level, a user can be created but that user has a certain access provision. And above (Fig. 5) a user named *jane* cannot be able to login since she does not have a 'create session privilege' which has now been granted to her as shown in the Fig. 6;

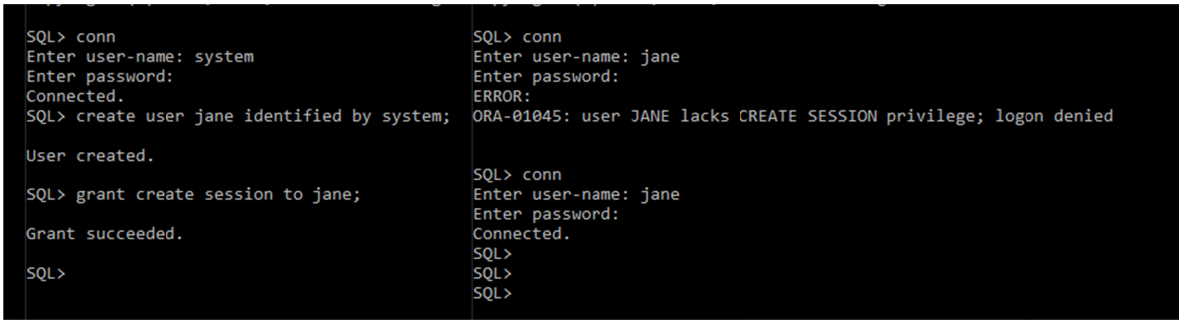


Fig. 6: Privilege levels (Research data, 2017)

From Fig. 6 it can be noted that the user *jane* has now been given 'create session privilege'. This clearly illustrates the running compliance and standard scores.

3.2 Requirements for an Effective DB Security Metrics

For a database metric to be effective and efficient the organization has to be able to fully comprehend the metrics, gain management support and approval, understand the exact information required of all the metrics, and conduct a regular review and update of the metrics.

3.3 Categories of database security metrics:

The National Institute of Standards and Technology (NIST) categorize metrics into three groupings under the Performance Measurement Guide for Information Security (NIST SP 800-55 Revision 1). The categories are:

i) *Implementation* – metric for showing progress in policy implementation, action plans and security controls.

ii) *Effectiveness and efficiency* – metrics used to track results of security control implementation.

iii) *Impact* – metrics used to show the impact of the information security program on the institution's mission, often done through quantifying of costs avoided or risk reduction achieved.

3.4 Sample situations of DB security metrics

Database security metrics can be implemented in a number of ways. For instance, an organization could note the number of false SQL server instances over a short period of time like a month, record a number of futile back-up attempts, take statistics of the percentage of total database access privileges with difficult passwords, record the time taken to evaluate and retrieve client data on a DB security event, and note the instances of systems compliance with regulatory and ethical standards

3.5 Comparison and variation of database security metrics for different entities:

The overall information security program of an institution or entity will determine the effectiveness of a particular metric. For instance, institution A issues a policy about all workstations data being encrypted and institution B has had the same policy for five years. Thus, after ten months, institution A having a metric about policy compliance would be more important that if B had the same as this has now become routine for B.

The process of ensuring database security should systematically be able to be planned, discover and assess, secure, monitored, protect and manage.

3.6 Importance of Database Security Metrics:

Metrics are very important to an information security unit in an organisation as they provide an insight concerning information security program efficacy, they let an organization benchmark their security investments against other organizations, they show the height of compliance to regulations, the metrics "gathering" process often leads to identification of security inconsistencies or holes, and indicate levels of risk and required mitigation strategies.

In order to put good database security metrics in place, it's important to ask questions such as, how difficult will it be to collect data meant to address a certain metric? what are the chances that the metric may be misconstrued? will regular review of metrics and update be conducted as needed?

4. DISCUSSION

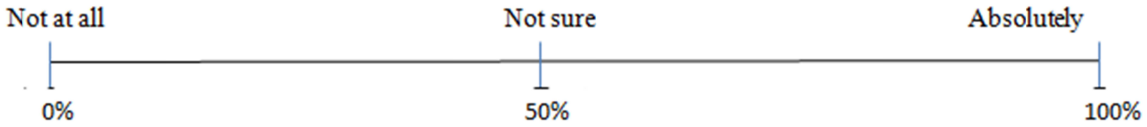
With the ever widening landscape of threats on databases, organizations have been forced eventually to change the way they work. The key factors that have driven database security metrics are money matters (return on investment), governance and management, risk mitigation, decision-making at all levels, sensitive business and customer data, need to comply with regulatory requirements, high profile data breaches experience by other organizations, legal and ethical responsibilities, and the need to find out how effective information security implemented is.

Therefore, in order to measure and report on database security issues, metrics include:

Metrics for losses that arise from security incident: It is worth to track and come up with all the losses from security incidences in order to establish a best case basis for management decisions. These costs include direct losses, investigative and corrective actions, legal action and may be measured or estimated, although losses arising indirectly might be difficult to measure but can at least be classified into high, low or medium. The security of database is a subset of all security incidents but the key concern is the failure of confidentiality, integrity and availability (CIA) of data. For example, a worm that causes a widespread network disruption. Costs associated with unplanned outages of vital database system to clean up the worm's damage can be accounted for as a database security failure as well as part of the costs of malware incidents.

Database security control costs metric: The security control of a database include controls that are specific to database, for example, database user authentication and encryption software and generally security controls like physical protection of servers in the data center. It might be possible to allocate the IT departments costs to security, operations, development and other categories, and within security to identify database security costs. High level summary metrics are perhaps the best than can be expected.

Confidence metrics: Managers and stakeholders may be surveyed regarding their confidence in database security for example; how confident are you that our database security controls meet the business needs? Please mark the following percentage scale at the appropriate point, in your opinion.



Comment e.g what has led you to this score? Have there been particular situations or incidents that influenced your decisions?

The metrics can be indexed to come up with a value to reveal the state of the organizations controls. Also graphing the accumulated database security losses over the course of a year, for instance, should highlight the peaks caused by serious incidents and provide opportunities to discuss the actions taken to prevent a recurrence.

5. CONCLUSION

In developing database security metrics, it is important to conduct a risk analysis of the risks and value of assets in the organization in accordance with their risk exposure. This exercise should be done across all components of an information system that includes people, information, network, system patches, system hardware and software, and the database servers. This will aid in coming up with suitable yet effective database security metrics for use in countermeasures against threats and vulnerabilities.

6. AREAS FOR FURTHER STUDY

It can be noted that database is the core of information and information systems. Therefore efforts in ensuring further survey into the index factor of database dependability would be a viable approach to confidence level attached to a database implementation and design.

7. REFERENCES

Al-Sayid, N. A., & Aldlaeen, D. (2013). *Database security -threats: A survey study*. In *Computer Science and Information Technology (CSIT), 2013 5th International Conference on* (pp. 60-64). IEEE.

Cavoukian, A., & Jonas, J. (2012). *Privacy by design in the age of big data*. Information and Privacy. Available at: http://gpsbydesign.org/wp-content/uploads/2016/07/privacy-by-design-in-the-age-of-big-data.pdf

Guimaraes, M. (2006). *New challenges in teaching database security*. In *Proceedings of the 3rd annual conference on Information security curriculum development* (pp. 64-67). ACM.

Murray, M. C. (2010). Database Security: What Students Need to Know, *Journal of Information Technology Education*, Volume 9, PP. 61-77. Available at: http://www. jite. org/documents/Vol9/JITEv9IIPp061-077Murray804. pdf

Razdan, R., & Bommakanty, S. (2001). *U.S. Patent Application No. 09/769,443*.

Cite this article:

Juma, J. and Makupi, D. (2017). Understanding Database Security Metrics: A Review. MIJSRP. Vol. 1, No. 1, Pages 40 - 48