Database Security through Risk Assessment

Rajani D. Singh
Researcher, RTMNU, Nagpur
Working in S.P. College,
Chandrapur

S.B. Kishor, Ph.D.
Head of Computer Science,
Sardar Patel Mahavidyalaya,
Chandrapur

ABSTRACT

Database Security is the foundation of the new Electronic Business, E-Commerce and other Business System including Intranet and Extranet Users. The Internet and E-Commerce uses have ballooned and India has become an emerging power in the IT Enabled Services field. As Internet accessing costs are falling user's increases and India ranking in terms of Internet users is raising fast.

Vulnerability hunts for the weakness in Database and generally concentrates on the database security problems which mainly arise due to the increasing number of users having various levels of access to the central as well as distributed databases. Database security requirements are dynamic in nature. Now a day, hackers beat network security by masking themselves as legitimate users. The intruders can penetrate systems with one of the legitimate access account. Generally they are not going to breaking down gates, but they can access each system with legitimate certificate. Hackers steal user's information from a home user's computer, tricking employees into breaking passwords or user names, or sniffing an ISP.

Some Techniques like Buffer Overflow, SQL Injection, Pharming, Bots and Trojan Horses are the terms who inject the problems in Database. Semantic Encoding, Vulnerability Assessment Scanner, Bound Checking and Intrusion Prevention are some techniques to solve the security related Problems of database distributed over the Internet.

Keywords

Distributed Servers, Virtualization, Risk Assessment, Vulnerability Assessment.

1. INTRODUCTION

The increase use of Mobile and Tablet Devices will be the source of increased security threats over the coming month. Also they encounter the Cyber-espionage, privacy violations and social networking attacks. To help DB Admin, Security Professional and to protect the database and avoid any crime scene, it is important to find out the different methods of attack, data theft and cover up technique. For that any Professional has to arm with good detective, understanding, technique and tools. Data that is secure in one country cannot say it is secure in another country. In the current cases where users uses cloud services. They don't know where their information is held. Users only have the benefit from Local law and jurisdictions.

Government, Research, Corporations and other Organizations keep large volume of data either in Database or in Data Warehouse which are not expected to be available to un-authorized users. And if anyone can access this data it must be unreadable and absolutely incomprehensive.

Generally observed problems with Database Securities are:

- Theft and Fraud
- Loss of Confidentiality
- Loss of Privacy
- Loss of Integrity
- Loss of Availability

2. HYPOTHESIS OF STUDY

Most of the Public Sites allows the users to see and use all information without logging in also many Social sites allows anybody to join without creating an account, in such cases any privileges are not given to users. Cases like User Virtualization and Cross Database Access are some striking area for study.

- Lack of an enterprise level security policy.
- Weak user security set-up
- Overall Piteous Database strategy
- Net connection problem
- Low speed accessing
- Awareness of internet applications and services
- Time consuming activity

3. SECURITY THREATS AND VULNERABILITY

Threat can be defined as the action to breach the security of system and Vulnerability can be defined as the high potential provided to the intruders to get access in system.

Different latest security threats are as follows.

i. Distributed Servers

ii. Virtualization

iii. Cloud Servers

Immersed as the face of new Technology.Crucial task to determine the attacks and to patch up the security holes in the Database.

In Distributed Servers, logical and physical separation exists between the client and server and the client/server system co-ordinates the work of both of these components and efficiently uses each one's available resources to complete assigned tasks. This separation of client and server provides an open and flexible environment for potential attack. The distribution of services in client/

server increases the susceptibility of these systems to damage from viruses, fraud, physical damage and misuse than in any centralized computer system. Whereas Virtualization or Cloud Servers faces problems like File Sharing between Hosts and Guests, Snapshots, Network Storage, Hypervisor, Virtual Machines, Separation of Duties, Administrator Access and Time Synchronization

4. RISK ASSESSMENT

The risk assessment process includes identification and evaluation of risks, risk impacts, and recommendation of risk-reducing measures. One of the methods for identifying risk is to create a risk item checklist like given below:

- Organizational and Management Practices
- Personnel Practices
- Physical Security Practices
- Data Security Practices
- Information Integrity Practices
- Software Integrity Practices
- Personal Computer Security Practices
- Network Protection Practices
- Incident Response Practices

5. RISK ASSESSMENT STEPS

- System Characterization
- Threat Identification
- Vulnerability Identification
- Control Analysis
- Likelihood Determination

6. OPEN SOURCE TOOLS FOR RISK AND VULNERABILITY ASSESSMENTS

Risk and vulnerability assessment determine systems that have been misconfigured or have not been fully patched. Very early on, in the emerging days of computer security, experts quickly realized the need for an automated tool to scan systems for known vulnerabilities and common misconfigurations. A number of tools were developed for this purpose. But the ones that have stood the test of time and have gained popularity are those that are regularly updated, because the number of security bugs discovered every week could simply overwhelm any small or medium-sized team that develops and maintains vulnerability assessment tools. Modern data centers deploy firewalls and managed networking components, but still feel insecure because of crackers. Hence, there is a crucial need for tools that accurately assess network vulnerability.

6.1 Vulnerability Assessment Tools

- **Nessus**
  Nessus is one of the most popular and effective tools for assessing vulnerabilities in a network. It works in a client-server architecture, wherein the server stores the database of vulnerabilities to be tested, accepts connections from clients and completes the actual scanning.
- **SATAN**
  The Security Administrator's Tool for Analyzing Networks (SATAN) was one of the earliest vulnerability assessment tools, and was developed by security expert Wietse Venema to audit the susceptibility of various UNIX operating systems to known vulnerabilities.
- **Port Scanners**
  Every application that provides a service to clients uses a port number. Most such services use well-defined port numbers. For instance, the HTTP service, which is used by web sites, runs on port 80. By determining the services running on various ports, the auditor can determine the many avenues of attack that an attacker might use against the system. Port scanning is the act of trying to connect to various ports on a given system and determining which ones respond to the request.

6.2 Network Auditing Tools

Network auditing consists of testing the security of the network elements within the system, such as firewalls and routers, as well as testing network parameters of the operating systems of the servers.

- **Hping2**
- **Firewalk**
- **Windows Network Testing**

6.3 Host-based Auditing Tools

Host-based auditing consists of scanning a system locally, and determining unpatched software and common misconfigurations. A host-based auditing tool is theoretically more comprehensive than a network-based vulnerability assessment tool simply because it has greater access to system information than a network-based tool.

- **COPS**
- **Tiger**

6.4 Forensics

Computer forensics deals with the investigation of a computer system that may have been compromised. The investigation is done by taking the affected system offline and is aimed at determining the attacker and his/her methodology, either for research or legal purposes. This is a vast field by itself with numerous articles and extensive research having being done on it.

- **The Coroner's Toolkit**
- **Lsof**

7. LIMITATIONS

Database cannot be defined as only an application that manages data and allows fast storage and retrieval of that data. Database Security is the renowned area whose main aim is to Protect Database against the Intentional as well as Accidental Threats.

Latest technologies like Distributed Servers, Virtualization and Cloud Servers immersed as the face of new concepts. So it is the crucial task to ascertain the methods of attacks and to patch up the security holes in the database. The attackers may be the Insiders or outsider so that some threats are easily prevented while others can do disastrous damage. Thus it consists of limit and scope of the investigation.

8. CONCLUSION

As the main aim of any research is to find out the truth which is hidden in the current trend and technology present in the Market or which is highly favourable among the Users. Database is defined as the organized collection of data used for one or more purpose which stores the Financial, Healthcare, Insurance, and Educational Data. Generally Database Administrator focuses on the Design Complexities of the Data Base to Provide the Consistent and Flawless service. That's why they cannot totally concentrate on the Security Strategies.

The Objective of this paper is to provide details of various Threats and Vulnerability over the Database Security. This paper focuses on the various Free Ware Risk and Vulnerability Assessment Tools available in Market who offers us to Security our precious Data from various potency Threat.

9. REFERENCES

[1] Ali Amer Alwan, Hamidah Ibrahim and Nur Izura Udzir, "A model for ranking and selecting integrity tests in a distributed database", international journal of information technology and web engineering, volume 5, issue 3. 1554-1045, pages 65-84

[2] E. Eugene Schultz, "Computer forensics challenges in responding to incidents in real-life settings, computer fraud & security", volume 2007, issue 12, 1361-3723, December 2007, pages 12–16

[3] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham, "Security issues for cloud computing", international journal of information security and privacy, volume 4, issue 2, 1930-1650, pages 39-51.

[4] Nigel Hawthorn, "Finding security in the cloud, computer fraud & security", volume 2009, issue 10, 13613723, October 2009, pages 19-20

[5] Robert L. Totterdale, Robert Morris University, USA, "Globalization and data privacy: an exploratory study", international journal of information security and privacy", volume 4, issue 2, 1744-1765. mohd alwi, najwa hayaati; fan, ip-shing, "information security threats analysis for e-learning", volume 73, 2010, springer-verlag berlin heidelberg, isbn 978-3-642-13165-3

[6] M.Tamer Ozsu, "Distributed Database System", pearson edu., fourth edition, 2004,81-7758-177-5, Delhi

[7] R. Paneerselvam, "Database Management System", Prentic hall in india, eighth edition, 2007, 978-81-203-2028-4, New Delhi

[8] R. Buyya, J. Broberg, "Cloud Computing Principals and Paradigms", wiley press, first edition, 2011, 978-0470887998, New York, USA

[9] Silberschstz, "Database System Concepts", Tata Mcgrawhill, fourth edition, 0-07-228363-7, New Delhi

[10] Silberschstz, "Database System Concepts", Tata Mcgrawhill, fifth edition, 2006, 0.07-124476-x, New Delhi

[11] Diane Barrett, Greg Kipper, "Virtualization and Forensics", Syngress, 2010, 978-1-59749-557-8,

[12] Whitehorn, "Insite Relational Database", Springer International Edition, second edition, 2003, 81-8128-052-0, New Delhi

[13] Wilbur Cross, "Investor Alert! How to protect your money from schemes, scams, and frauds", Andrews and Mcmeel, 1988, 9780875022307