Database Tamper Detection and Analysis

Shagufta Rajguru
F.C.Rodrigues Institute of Technology (faculty)
K.J.Somaiya College of Engg (student)

Deepak Sharma
K.J.Somaiya College of Engg

ABSTRACT
Database as an enterprise data information aggregation is a core component its security is essential. The data and the metadata when exposed to the outside world may endanger the security of the DBMS. Therefore securing data and assuring that the database should be accessed by authorized users is necessary.

In this study we have understood the architecture of oracle 10g [1] and studied different queries that can be fired to retrieve the facts and details form the system log files and redo log files from the oracle database. A proposed design of a forensic tool that will detect the tamper on the content of the database and analyze when, where and who did the tamper on the database is stated.

Keywords
Database, Oracle 10g, database tamper, database forensic

1. INTRODUCTION

1.1 Database Forensic
Database Forensics [2] is a branch of digital forensic science relating to the forensic study of databases and their related metadata. A forensic examination of a database may relate to the timestamps that apply to the update time of a row in a relational table being inspected and tested for validity in order to verify the actions of a database user.

1.1.1 Database Tampering [3][13]
For many organizations, if data were to be maliciously changed, whether by an outsider or by an inside intruder, it could cause severe consequences for the company. Possibly even for their clients as well. There are many reasons why someone might want to tamper with data.

1.1.2 Introduction to Digital Forensic Analysis
Digital forensics [3] is the process of uncovering and interpreting electronic data for use in a court of law. The goal of the process is to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying and validating the digital information for the purpose of reconstructing past events.

The entire investigation process can be divided into four phases.

- **Identification:** In this phase it collects the information of the compromised system. System Configuration, software running on it, user profiles etc.
- **Collection Phase**: Collects the evidence from the compromised system. Evidence is most commonly found in files and Databases that are stored on hard drives and storage devices and media. If file deleted, recovering data from the deleted files and also collects evidence file deleted files.
- **Analysis phase**: Analyze the collecting data/files and finding out the actual evidence.
- **Report phase**: The audience will be able to understand the evidence data which has been acquired from the evidence collection and analysis phases. The report generation phase records the evidence data found out by each analysis component. Additionally, it records the time and provides hash values of the collected evidence for the chain-of-custody.

1.2 Background and Motivation
As a database forensic examiner the concern is to analyze the data to identify who, where .when and how tampered the data. This issue is still not solved.

The development of data mining and Internet technology increases the rate of the tampered database, which drives improvements on authentication of database integrity. Many researchers have built a lot of reliable mechanisms for database content protection with cryptography techniques. Divada proposed the concept of database encryption [4] system with subkeys to enforce database security, which is based on record oriented and encrypted process individually for each attribute. Hwang and Yang presented a multilevel database encryption/decryption system with sub keys. Encryption techniques make sure that the encrypted dataset is meaningless to the attacker. Once the dataset is decrypted, which is no longer under protection, the dataset is in the clear conditions. Until now, digital watermarking, a new emerging technology, embeds an invisible signal into the dataset and implementing dependable solution to protect digital data from illicit copying and manipulation. Digital watermarking has been extensively studied in the content of multimedia data for the purpose of ownership protection and authentication. It has been widely applied to multimedia data, such as image, video, audio, and so on. The objects are usually based on the digital watermarks of inserting into the protected data. The watermarking schemes will produce slight errors while it is embedded into the watermarked media. These designated errors are called marks, and all marks are jointly organized into the Watermark.

The organization of the report is as follows. It discusses about the steps how to investigate the evidence and from which location of the oracle database architecture it can be collected. The section 2 discusses about the problem statement and the description of various modules of the project. In section 3 the design implementation of the first module “modified table” is discussed in details. Finally, section 4 presents concluding remarks and outlines future work.

2. PROBLEM STATEMENT AND DESIGN SPECIFICATIONS OF THE MODULES

2.1 Problem Statement

To design a database forensic tool whose task is to detect the tamper on a database object, analyze the integrity of object to what extent it was modified, determine the attacker's activities and also identify who, when and where logged into the database.

2.2 Modules of the Project

- Modified Table
- Deleted Table
- Unauthorized Access Table

2.3 Proposed Design

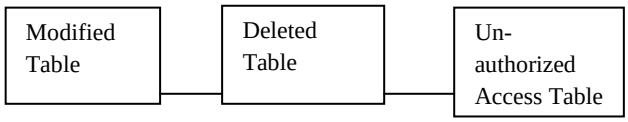

Fig 1: Proposed Block diagram I

3. PROPOSED IMPLEMENTATION AND DETAILS

According to the modules stated above, the implementation of the first module is undertaken that has the following sub sections.

3.1 Modified Table

3.1.1Authentication Investigation

One would try to investigate the authenticated and unauthenticated users using three basic steps as mentioned below in order to collect evidences.

- Obtain the DBA_Roles
- Obtain the DBA_Privileges
- Identify Enumeration Attack

3.1.1.1 Obtain the DBA_Roles

Investigation under this heading reveals the information about different dba_roles defined for the database which are to be investigated. This information can be revealed using the query given below.

SQL>SELECT * FROM dba_role_privs;

With the list of different roles defined in the database we can understand the official roles assigned to different users.

3.1.1.2 Obtain the DBA_Privileges

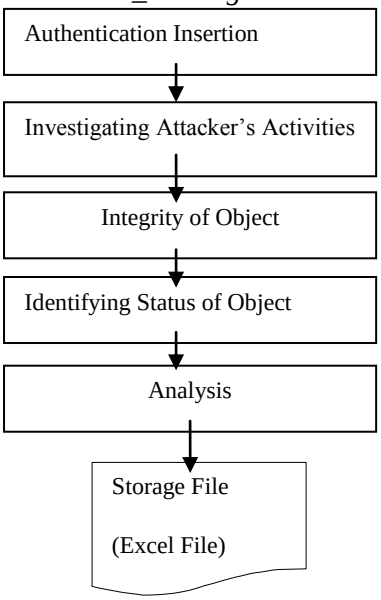

Fig 2: Proposed Block Diagram of Modified Table

DBA_Privileges gives the information about different privileges given to the roles defined in the database. With this information one can understand the rights assigned to each user and hence analyze the user who has violated the privilege. This information can be obtained with query mentioned below.

SQL>select grantee, privilege, admin_option from dba_sys_privs where privilege like '%AUDIT%';

3.1.1.3 Enumeration Attack

This stage is used to spot user enumeration attack. During Oracle authentication the client presents their username to the server in one packet. If the username exists in the database then the server issues a session key and the client sends over their encrypted password in a second packet. If the user does not exist the server sends back an error: ORA-01017: invalid Username/password; logon denied. Due to this difference in behavior, it's possible for an attacker to determine whether a given user account exists or not. If the account does not exist an entry is created in the audit trail with a 1017 return code. We can identify the unsuccessful attempts of the attacker using following query.

SQL> SELECT USERID, ACTION#, RETURNCODE, TIMESTAMP# FROM SYS.AUD$;

3.1.2Investigating Attacker's Activities

After dealing with authentication investigation we need to understand the activities performed by the attacker. To do so different steps are listed down:

- Predicate
- Last accesses Time
- Recently accessed table

3.1.2.1 Predicate

This step is used find out how many times the 'where' clause was used in SQL queries on objects (for example salary table) in the database and it was executed by whom. The query is given below.

SQL>SELECT C.TIMESTAMP, O.NAME, C.INTCOL#, C.EQUALITY_PREDS FROM COL_USAGE$ C, OBJ$ O WHERE C.OBJ#=O.OBJ# AND C.EQUALITY_PREDS > 0;

3.1.2.2 Last Access Time

This investigation gives us the information about what was last access time of the sql query and it was accessed by which user. This is valuable information for a forensic analyst. It can be obtained with the following query.

SELECT LAST_ACTIVE_TIME, PARSING_USER_ID, SQL_FULLTEXT FROM V$SQL;

3.1.2.3 Recently Accessed Table

This investigation gives us the information about which table which was accessed recently by the user. From this information we will understand whether the salary table was accessed recently. The query executed to retrieve this information is stated below.

SQL>SELECT OWNER, NAME FROM V$DB_OBJECT_CACHE WHERE NAMESPACE ='TABLE/PROCEDURE' ORDER BY 1

3.1.3 Integrity of Object

Not only attacker's activity should be investigated the integrity of the object should also be checked. This step will give us information about the state of the object. This step may become the milestone in the process. To obtain the integrity of the object some few steps are defined below.

- State check table over time
- Checksum of data
- Compare checksum

3.1.3.1 State Check Table Over Time

The integrity of the table (for example salary table) by converting the System Change Number (SCN) of each row of the table into its timestamp can be checked. With this information one can obtain the time when each row of the table was changed. To do so the following query can be used.

SQL>SELECT SCN_TO_TIMESTAMP(ORA_ROWSCN) FROM scott.salaries;

3.1.3.2 Checksum of Data

The information obtained from this step of investigation will help us to check the state of the table has not changed from the previously known state. One needs to first create the checksum of the table. It can be done with the help of following query.

SQL>select DBMS_SQLHASH.gethash('select 1 from scott.salaries', 2) from scott.salaries;

3.1.3.3 Compare the Checksum

At this stage the checksum generated at the earlier step is compared with the recently generated checksum. If a result set is returned then the state of the table data is the same as the previous known checksum. If "no rows" are selected then the state of the table's data has changed from that represented by the previous known checksum. The query used to obtain this information is shown below

SQL>select utl_raw.cast_to_raw(DBMS_SQLHASH.gethash('select 1 from scott.salaries',2)) from scott.salaries)intersect(select utl_raw.cast_to_raw('6656611BC92D07CCEA713CDFA32AB1A22') from scott.salaries);

3.1.4 Identifying Status of Object

After performing the investigation at earlier stage now at the final stage one needs to analyze that actually who did the attack, when was it done and what exactly was attacked. Hence we divide his section into three parts

- Who logged on
- When logged on and
- What logged on

The details of each part are explained as follows.

3.1.4.1 Who Logged On

To identify who logged the system the following query is used.

SQL>SELECT USERID, COMMENT$TEXT FROM SYS.AUD$;

3.1.4.2 When Logged On

To identify when the attacker logged on to the system a timeline should be created which will highlight all the activities of the attacker. This information can be obtained using the following query.

SQL>SELECT SCN, TIMESTAMP, USERNAME, TABLE_NAME, OPERATION FROM V$LOGMNR_CONTENTS;

This query obtains the information from the logminer tool.

3.1.4.3 What Logged On

This is the final step of investigation where the investigator will come to know exactly what was tampered. Following query is used to obtain this information

SQL>select username, seg_owner,operation,sql_redo,sql_undo from v$logmnr_contents where operation ='UPDATE' and USERNAME='SCOTT';

From the query this information is also retrieved with the help of logminer tool.

3.1.5 Analysis

In this particular section a graph can be generated depending on the access time and the no of users accessing the database. From the graph one can identify who has accessed the database for the longest time and accordingly the analysis can be made as to who tampered the database.

4. CONCLUSION

To violate the security of the database there are attackers to identify the vulnerabilities in the security methods of the system and hence attack the system and gain the unprivileged information. Then comes the role of forensic analyst who should have a thorough knowledge of the basics of a database and also the information about the

database on which he is going to perform the analysis. The forensic analyst should also be able to think from the attacker's point of view. Based on different cases, the digital evidences can be collected from the specified locations. If the intensions of the attacker are known identifying the attacked location may be easier.

Therefore in this paper a proposed design of a tool that will try to investigate the integrity of the object, attacker's intentions and time and location when the attack was done on that object is given.

5. FUTURE SCOPE

As the future scope of this project we would like to implement the following modules. All the modules are independent from one another.

- Deleted Table
- Unauthorized Access Table

The liability of the evidences should be checked. The chain of custody should be developed.

6. REFERENCES

[1] Oracle Database 10g DBA Handbook

[2] http://www.techopedia.com/definition/27805/digital-forensics

[3] Oracle Database Forensics using LogMiner Option 3 - Perform Forensic Tool Validation GCFA Assignment Version 2.0 Paul M. Wright - GSEC, GCFW, GCIH January 10th 2005 from London June 2004 Conference

[4] Tamper Detection in Audit Logs Richard T. Snodgrass, Shilong Stanley Yao and Christian Collberg University of Arizona Department of Computer Science Tucson, AZ 85721-0077 USA frts,yao,collbergg@cs.arizona.edu

[5] Litchfield, David. "Oracle forensics part 1: Dissecting the redo logs."NGSSoftware Insight Security Research (NISR), Next Generation Security Software Ltd., Sutton (2007).

[6] Litchfield, David. "Oracle forensics part 2: Locating dropped objects."NGSSoftware Insight Security Research (NISR) (2007).

[7] Litchfield, David. "Oracle Forensics: Part 3 Isolating Evidence of Attacks Against the Authentication Mechanism." NGSSoftware Insight Security Research (NISR) (2007).

[8] Litchfield, David. "Oracle forensics part 4: Live response." NGSSoftware Insight Security Research (NISR), Next Generation Security Software Ltd., Sutton(2007).

[9] Litchfield, David. "Oracle forensics part 6: Examining undo segments, flashback and the oracle recycle bin." NGSSoftware Insight Security Research (NISR), Next Generation Security Software Ltd., Sutton (2007).

[10] Oracle Forensics Part 7: Using the Oracle System Change Number in Forensic Investigations David Litchfield [davidl@ngssoftware.com]

[11] Shweta Tripathi,Sindhu. K. K , Dr.B.B. Meshram "Digital Forensic Investigation on File System And Database Tampering " IOSR Journal of Engineering (IOSRJEN) www.iosrjen.org ISSN : 2250-3021 Vol. 2 Issue 2, Feb.2012, pp.214-221 www.iosrjen.org 214 | P a g e

[12] Shweta Tripathi, Bandu Baburao Meshram "Digital Evidence for Database Tamper Detection" Journal of Information Security, 2012, 3, ***-*** Published Online April 2012 (http://www.SciRP.org/journal/jis)