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.

References

- Oracle Database 10g DBA Handbook
- http://www.techopedia.com/definition/27805/digital-forensics
- 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
Database Tamper Detection and Analysis

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

Index Terms

Computer Science Databases

Keywords

Database Oracle 10g database tamper database forensic