Audit Trail

Priyanka Nikalje
Thakur Institute of Management Studies,
Career Development and Research (TIMSCDR)
Mumbai, India

Gauresh Lotlikar
Thakur Institute of Management Studies,
Career Development and Research (TIMSCDR)
Mumbai, India

Manish Mishra
Thakur Institute of Management Studies,
Career Development and Research (TIMSCDR)
Mumbai, India

Shirshendu Maitra
Assistant Professor
Thakur Institute of Management Studies, Career Development and Research (TIMSCDR)
Mumbai, India

ABSTRACT
In today's IT world computer systems are vulnerable by both insiders (i.e. employees) as well as penetration by outsiders (or attackers). Also there are evidences showing the growing number of incidents reported in the press for such abuse. Closing all security loopholes from today's system is infeasible, whereas no combination of technologies can prevent legitimate users from abusing their authority in a system, auditing in viewed as the last line of defense. But auditing a large amount of data is not a feasible option hence what is needed is automated tools to analyze the vast amount of audit data for suspicious user behavior. This paper presents audit trail analysis technique and intrusion detection systems that have emerged in the past several years.

Keywords
System log, audit, trail

1. INTRODUCTION
The last few years have been a sudden and growing interest in automated security analysis of computer system audit trails and in system for real-time intrusion detection. There is a growing number of research activities devoted to the audit trail, and some operational systems and even a few commercial products have appeared.

Audit trail is also known as audit log, it is a document that has records of all events concerned to a particular event that has occurred. This document contains information related to the event like resources accessed, its destination, source address, a timestamp and the information regarding the user who performed the event.

Auditing is the monitoring and recording of selected user database actions, from both database users and non-database users. Logs can contain huge information about the events taking place within the systems and networks. Auditing can be based on individual actions, such as the type of SQL statement executed, or on combinations of data that can include the user name, application, time, and so on. Both successful and failed activities can be audited.

To use auditing, first enable it, and then configure what data should be audited in database. The actions that are audited are recorded in either data dictionary tables or in OS files.

It is an effective method of enforcing strong internal controls, and to enable you to monitor business operations, offering us the important layer of security and transparency. And help find any activities that may deviate from the organizations policy.

2. WHAT TO LOG
Wherever Times For each system monitored and likely event condition there must be enough data logged for determinations to be made. At a minimum, it is needed to be able to answer the standard who, what and when questions.

The data logged into the audit trail must be long enough to answer questions, but not indefinitely. Storage space costs money and at a certain point, depending on the data, the cost of storage is greater than the probable value of the log data.

The same can be said for costs associated with performance degradation that the log analysis tools suffer if the data sets are simply allowed to grow indefinitely.

3. HOW TO AUDIT PERIODICALLY
Check for objects and system permissions: - Check views, stored procedures tables, etc. A situation of compromise would occur in case of any changes.

New database installations search: -Third party products are able to install database servers and new installed servers can be installed with blank or weak passwords, un-patched etc. New database installations should be detected and secured or should be removed.

Look for users with DBA privileges: - This does assist to elevate privileges, detecting intrusions, etc.

Audit database configuration and settings: -Your databases could be used to an open attack if security configurations or settings are changed, for instance, by a System upgrade, patch, etc. If they change and there was not a system upgrade then that indicates a compromise.

Check changes for database system objects: - If you detect a change in a system object and you haven't applied a fix or upgrade to your database server it signifies that a root kit is present.

4. AUDIT TRAILS AND LOGS
A system can maintain several types of audit trails simultaneously. The types of audit records are as follows: -

Event-oriented log- contains records giving detailed description of system, application or user events. In other words, it has sufficient information about the event occurred as well as who and what caused those events to occur. In general, time the event happened, the ID of the user related with the event, the program or command used to commence the event, and the result. The limitations come from their incapacity to discover the transactional dependencies between

Keystroke Monitoring-It is a special case of audit trails. Keystroke monitoring is the process used to record or view both the keystrokes entered by a user and the computers response during hat interactive session. It is conducted in an effort to protect system and data from intruders who access the systems without authority or in excess of their assigned authority. Hence monitoring the keystrokes can help repair the damage caused by intruders.

5. WHY TO USE AUDITING

Enable accountability for actions-this refers to actions taken in a particular schema, table, or tuple.

Notify about unauthorized user-an unauthorized user could be damaging the data. Hence reviewing of user authorization must be done.

Detect suspicious activity- if a user is deleting data then a security administrator might decide to audit all connections to the database and all successful and unsuccessful deletions in the database.

Restrain Users- if a user (or intruders) performs an inappropriate action.

Monitor specific database activity: this helps to gather information about which tables are being accessed, updated and even operations performed at peak times.

6. AUDIT EVENTS

System audit records are generally used to monitor and fine-tune system performance. It enforces certain aspects of policy such as access to files and system itself. If special accesses are to be used to later configuration files the system must then generate audit records whenever such accesses are used.

Application audit trails provides bigger level of recorded detail. It may be used to discern flaws in applications, or violations of security policy committed within an application. When an application is critical it is desirable to record certain details specific to each use.

User audits records are generally used to hold individuals accountable for their actions i.e. it monitors and logs user activity in an application or system by recording events initiated by the user such as access of a file, record or data. It exposes different security violations raging from simple browsing to attempts to plant Trojan horses or gain unauthorized privileges

7. AUDITING TYPES

Design your auditing strategy to collect information that you need to meet compliance requirements, but being sure to focus on activities that cause the greatest security concerns. Types of auditing are as follows:

Standard auditing- in this you audit SQL statements, privileges, schema objects, and network activities. The generation and insertion of an audit record is independent of a user transaction being committed. Even if a transaction is rolled back, the audit trail record remains committed.

Operating system Audit Trail- operating system file can be created using alternative standard audit records and that can include following data: -

- Audit records generated by OS
- Database audit trails
- Database actions that are always audited
- Audit records for administrative users

It reduces the likelihood of a denial-of-service (DoS) attack. It is easy to secure the audit trail. Writing an audit trail to an OS file results, in the least amount of overhead on database.

Syslog audit trail-Potential security vulnerability for an OS audit trail is that a privilege user can modify or delete database audit records.

8. TOOLS FOR AUDIT TRAIL ANALYSIS

Many types of tools are available in the market not only to help reduce the amount of data contained in audit records, but also to distill useful data from the raw data. Some of the types of tools are as follows:

Audit reduction tool is the preprocessors designed to reduce the volume of audit records to facilitate manual review. Before a security review, these tool help remove many audit records known to have little security significance. This alone may cut in half the number of records in the audit trail. These tools generally remove records generated by specified classes of events, like records generated by nightly backups may be removed.

Trends/variance-detection tools look for peculiarity in user or system behavior. It is possible to construct more sophisticated processors that monitor usage trends and detect major dissimilarity

9. CHALLENGES FACED IN LOG MANAGEMENT

The most common problem faced is effectively balancing the ever-increasing log data and limited amount of management resources. The other most commonly faced challenges by organizations are: -

Initial generation of logs-A single log source can generate multiple logs, and each log source contains certain pieces of information such as user ID, IP address, username, before data and after data, timestamp. Hence to facilitate analysis organizations need to implement automated methods of converting logs with various content and formats to a standard representation format.

Log protection- Since log contains detailed and sensitive information of system and network; they can be breached by both authorized and unauthorized means. This could cause different types of impact, including allowing malicious activities to go unnoticed and manipulating proofs to conceal the identity of a malicious party.

Log Analysis- Generally administrators responsible for performing analysis of logs are not trained efficiently. Also they usually do not receive tools for the process of analysis. Administrators consider the job of analysis to be monotonous and providing less benefit for time amount of time invested.

10. BENEFITS

There are various reasons available for usage of audit trail out of which few are:

Accountability: if a file goes missing or some important information gets deleted, then audit trails will simply help us find who was responsible for it hence eliminating suspicion and creating a work friendly environment

Compliance: This will help manager ensure that the management processes going on are all compliant with standard regulations.

Regulate workflow: In big organization, multiple people work on a single project, this in turn makes it complicated to manage which employee has been responsible for what part of the project. Hence using audit trail can make working on project easy all the way down to the basic task flow.

Better output: When people know their work is being monitored they tend to work better, so this encourages the working team members to do their best. And this in turn also gives management the chance to identify its employee's needs.

Security: Having detailed information about business data can help organization monitor data for a potential security breaches or internal misuse of information, preventing fraud.

Reconstruction of events: Knowledge from the previously occurred events can help in avoiding future outages. This can simply be done by recreating the same situation and finding feasible solutions i.e. the recovery process.

11. MEETING THE CHALLENGES

Despite many challenges in log management there are few key practices which can help avoid and even solve the challenges which are:

Prioritize- throughout the organization prioritize the log management by defining its requirement and goals based on the applicable laws, regulations, organizational policies, and application/data sensitivity. This will in turn help organization reduce its risk with resources and time needed.

Establish-Policies and procedures must be established for log management such that they meet the laws and regulatory requirements. Periodic audits are the most common technique to confirm the establishment whereas testing and validation and can further confirm that the adopted procedures are performed properly.

Secure-To preserve the integrity of data from accidental or intentional changes organizations must create components of log management infrastructure and also determine how these components interact.

Support-Necessary training must be given to the relevant staff regarding their responsibilities as well as skill instruction for the needed resources i.e. provides adequate support for all staff with log management responsibilities.

12. CONCLUSION

From the new methods of database audit trials analysis numerous knowledge of a student about his/her academic performance can be gathered. Data to any organization or Institution is a most important property. Protection of crucial data is always a tough task for an organization at any stage. Databases are most favourite and easy target for attackers because of the information it contains and its volume. Database can be accommodated in several ways. Different types of attacks and threats are there today from which a database should be protected.

13. REFERENCES

[1] http://www.academypublisher.com/proc/isnns10/paper/isnns10p275.pdf

[2] http://www.lexjansen.com/pnwsug/2004/ExtractingDatafromOracleintoSAS-LessonsLearned.pdf

[3] https://support.sas.com/training/tutorial/el/libsppg3_at.pdf

[4] http://www.atis.org/glossary/definition.aspx?id=5572

[5] http://www.datamation.com/columns/article.php/3578916/The-Importance-of-Audit-Logs.htm

[6] http://csrc.nist.gov/