Scientific Journal of Impact Factor (SJIF): 4.14

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 3, March -2016

An Effective Study on Database Intrusion Using Log Mining

Pooja Prasad[1], Reshma Charbhe[2], Dinesh More[3], Prof. S. G. Shaikh[4]

[1,2,3,4] *Department Of Computer Engineering, SIT College of Engg., Lonawala, Pune*

Abstract *— In database system because of insider misuse there is dangerous excruciating security problem. But today's scenario, more focus is given to external attacks because it is more visible, so some present technology are Intrusion Detection System(IDS) mechanism with Role based Access Control (RBAC). In this methodology permission are associated with roles and then intruder who is holding a specific role and system, efficiently determine role intruder but problem with it is that for extending Role base access proper planning is crucial and also effective when roles are carefully design. Next Technique is IDS using data mining. In which algorithm is develop for finding dependencies among the important item in Relational Database System (RDBMS), any transaction which does not follow dependencies are indentified as malicious, it also identify modification of sensitive attribute efficiently but disadvantage is that the high sensitivity attributes are usually access less frequently. There may not be any rule for such attribute. So, to overcome this flaws this paper intrudes idea of Log mining using intruder detection using comparative analysis We model users access patterns by profiling to keep track of users' usage habits as their forensic features and determines whether a valid login user to system or not.*

Keywords- *Data mining, Insider attack, Intrusion detection and protection, System call (SC), Users' behaviors.*

I. INTRODUCTION

The need for secure data storage has become a necessity of our time. In the era of globalization and dynamic world economies, data outsourcing is inevitable. Security is major concern in data outsourcing environment, since data is under the custody of third party service provider. In present systems, third party can access & view data even though they are not authorized to do so or even when the data is outsourced to the auditors or allow the employee of the organization to do the updating in the database. There are certain many such cases occurred in financial & insurance sector where the data is been tampered by the auditors or by the employees of the organization itself. It will easy for the admin to find out unauthorized user, if attacker trends and pattern is identified also will able to see most attacking parts. Almost all present systems which uses concept like intrusion detection (IDS) using packet sniffer [1],IDS using IP trace back [2], Role Base Access Control (RBAC) [3] or using dependency rule mining algorithm [4].In IDS mechanism with role based access control (RBAC), ID is stand on the concept that the result of database mining is stored in log files. And with the help of this result the user profile are created, which illustrate the normal behavior and from this, identify the intruders. So, this paper presenting idea of “An effective study on database intrusion using log mining” which eventually ease as the process by taking input as log file traces and perform the operation by using concept like IDS using Packet sniffer [1], IDS using IP trace back [2], RBAC [3] weighted dependency algorithm [4], and giving output as which transaction id is tampered?, what fields are tempered?, who did the tamper?, when did the tamper?.

II. LITERATURE REVIEW

As the previous sections reveals many methodology for “An effective study on database intrusion using log mining” but even though there is a huge gap to meet the perfection so as the step towards this, the paper try to grasp many concept so that new and efficient system can be proposed. The detail studies are as follows [1] Introduce method of IDS using packet sniffer which uses software application hat use a network adapter in promiscuous mode to capture all network packets that our sent over a local area network. By consider packet head field and packet content, all traffic over network analysis by IDS which set Ethernet card in primacies mode .Sniffer which is put inside of firewall it detects internal attack. [2] Explain the IDS using IP Trace back, it uses the logging method for carrying out trace back and resolve data security system, origin of devastation to network is search by IP trace back. [3] Introduce an idea of intrusion detection using RBAC. In this scheme, role information was available in the log records, we used it for training a classifier permission are given according to roles, IDS system determine role intruder when it is holding a specific role, by grouping several user rather than individual user, and he has abnormal behavior. And [4] describes the way of novel weighted data dependency rule mining algorithm, based on pattern of submitted query the algorithm mines use. Profiles and find out dependency among the data items. In which data dependency is also called access correlations. At the time of mining dependency rule the algorithm consider the sensitivity of attribute. This algorithm also capture any changes are made in sensitive attributes quickly. It also gives extension to the (ER) Entity- Relationship model to get the levels of sensitivity of the attributes But all this methodologies have some threats like in [2] IDS using IP trace back Is that it required long time for the two technique that is used after violation which are Proactive and mass storage data. IDS using RBAC [3] have some of the problem such as when in log records there if is no role information is available, and then log profile creation is totally unsupervised. One Another important issue in IDS using RBAC [3] is to capture the normal user behavior it maintains sub-profiles within a role profile is a more complex. Another threats in [4] host-based sensors do not do any packet level analysis. Instead, they monitor system level activities.

III. PROPOSED SYSTEM

This project propose the approach to ID is based on mining database traces stored in log files. In this Project, we present a new technique for identifying malicious database transactions. Are ideal for profiling data correlations for identifying malicious database activities. The result of the mining process is used to form user profiles that can model normal behavior and identify intruders. In this paper proposed a novel solution to overcome the problem of tamper detection by Log mining approach. Log files are the unalterable file in runtime, which are automatically created by the Web servers to have trace of the transactions by any web applications. By mining these log files and getting desired transaction trace from them, which we can consider as master data .By comparing this master data with the tampered data base if there is any difference between them we can detect tamper detection. Using the Log Mining algorithm, the administrator can extract the specific log files, which will help to compare the original database and the modified copy of database. If the changes made are legal or the same as expected then there’s no intrusion in the database. If the changes made are illegal then intrusion is detected and action can be taken.

IV. Mathematical Model

1. LOG FILE COPIER: (Here we cannot read Log file in run time as it is being using by web server, so we copy its content on that instance into a text file)
Set C:
C0= Get the path of Log File
C1=Read the content of log file
C2=Copy to a new .txt file in specified path

2. LOG CONTENT READER: (Here we read the log file content copied in Temporary .txt file and then store in a String object)
Set l:
L0=Get the path of copied log file in .txt
L1=Read the content and store in a String object

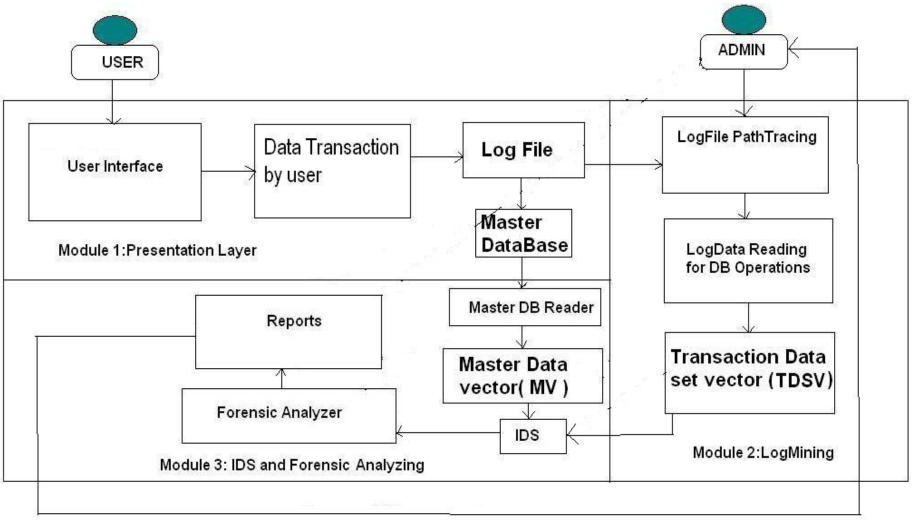
3. TRANSACTION DATA SET OBJECT MAKER: (Here we mine the String object of Log file and then make a object vector which consists of Data transaction Details)
Set T:
T0=Get Log String Object from L1
T1=Check for the Transaction trace in Log Object
T2=Make data set object vector
4. MASTER DATABASE OBJECT GENERATOR: (here we Read the Database and then get its content in an object vector)
Set M:
M0=Read the Database table
M1=Store the table content in Master Object Vector

5. INTRUSION DETECTOR: (Here we take two objects, one from Master database and another from Transaction Database and compare both the objects. If any indifference found then we consider as Intrusion happen and declare details of result in an .txt file)
Set I:
I0=Get Data Set object Vector from T2
I1=Get Master Object vector from M1
I2=Compare two vectors

I3= Check for any indifference and spot as intrusion
I4= Declare details in a result file which is in .txt file

Output: The output will be the detect the intrusion attack.

V. SYSTEM ARCHITECTURE



VI. CONCLUSION

As this complete paper narrates the different methodology on "An effective study on database intrusion using log mining" but none of the system or methodology are seems to be perfect so this paper as a width introduce idea of log mining using comparative analysis and intrusion report. To keep tracks of user's uses habits we record access pattern by profiling as there forensic features and find out it is a valid user or not.

ACKNOWLEDGMENT

We might want to thank the analysts and also distributers for making their assets accessible. We additionally appreciative to commentator for their significant recommendations furthermore thank the school powers for giving the obliged base and backing.

VII. REFERENCES

[1] **"**Network traffic analysis and intrusion detection using packet sniffer", M. A. Qadeer, M. Zahid, A. Iqbal, and M. R. Siddiqui, in Proc. Int. Conf. Commun. Softw. Netw., Singapore, 2010, pp. 313– 317

[2] "H. S. Kang and S. R. Kim, "A new logging-based IP trace back approach using data mining techniques" H. S. Kang and S. R. Kim ," J. Internet Serv. Inf. Security, vol. 3, 2013

[3] "Intrusion Detection in RBA Cadministered Databases" Elisa Bettino, Evimaria Terzi, The VLDB Journal, volume 1, 2 April 2011.

[4] "Database Intrusion Detection using Weighted Sequence Mining", Abhinav Srivastava, Shamik Sural and A.K. Majumdar, journal of computers, vol. 1,

[5]S. Gajek, A. Sadeghi, C. Stuble, and M. Winandy, "Compartmented security for browsers or how to thwart a phisher with trusted computing,"in *Proc. IEEE Int. Conf. Avail., Rel. Security*, Vienna, Austria, Apr. 2007, pp. 120–127.

[6] C. Yue and H. Wang, "BogusBiter: A transparent protection against phishing attacks," *ACM Trans. Int. Technol.*, vol. 10, no. 2, pp. 1–31,May 2010.

[7] Q. Chen, S. Abdelwahed, and A. Erradi, “A model-based approach to self-protection in computing system,” in *Proc.* ACM Cloud Autonomic Computer. *Conf.*, Miami, FL, USA, 2013, pp. 1–10.

[8] F. Y. Leu, M. C. Li, J. C. Lin, and C. T. Yang, “Detection workload in a dynamic grid-based intrusion detection environment,” J. Parallel Distrib.Comput., vol. 68, no. 4, pp. 427–442, Apr. 2008.

[9] H. Lu, B. Zhao, X. Wang, and J. Su, “DiffSig: Resource differentiation based malware behavioral concise signature generation,” Inf. Commun. Technol., vol. 7804, pp. 271–284, 2013.

AUTHORS

Pooja Prasad, student of BE Computer Engineering Sihngad Institude of Technology, Lonawala, Pune

Reshma Charbhe, student of BE Computer Engineering Sihngad Institude of Technology, Lonawala, Pune

Dinesh More, student of BE Computer Engineering Sihngad Institude of Technology, Lonawala, Pune