Internal Intrusion Detection and Protection System

[#1]Pratiksha Jadhav, [#2]Pooja Bhondave, [#3]Pratiksha Chavan, [#4]Sneha Dhere,
[#5]Prof. A. B. Gadewar

[1]jadhavpratiksha1996@gmail.com
[2]poojabhondave6@gmail.com

PDEA's college of Engineering, Manjari (BK), Hadapsar , Pune-412307, India.

***Abstract*:**

To authenticate users most computer systems use user IDs and passwords. However, many people share their login patterns with colleague and request these colleague to assist tasks. Insider attackers, the valid users of a system who attack the system internally, are hard to detect since most intrusion detection systems and firewalls identify and isolate malicious behaviors launched from the outside world of the system only. In this paper, a security system, named Intrusion Detection And Protection System, is proposed to detect insider attacks at SC level by using data mining and forensic techniques. The IIDPS creates users personal profiles to keep track of users usage habits as their forensic features and determines whether a valid login user is the account holder or not by comparing his/her current computer usage behaviors with the patterns collected in the account holders personal profile and profile image.
It also stores the file backup which is deleted, updated, modified by the attackers. IIDPS system provides security to the log files which are send over the network and it also provide security to the data stored in database.

Keywords- Data mining, insider attack, intrusion detection and protection, system call (SC), users' behaviors.

I. INTRODUCTION

In proposed system we are detecting the intrusion through many thing like integrity, checking currently running processes, by key log, etc. These all activities are performed by user. The first activity is file integrity. We are detecting intrusion through file integrity. In file integrity concept if any user delete the file or modify file or insert file into specific directory then by using our system we can detect it. If any file delete or modify of insert in to specific folder then that file will save in folder which is specified by client. Then file integrity log send to server. Server send the integrity of that file to the clients email id. So that client will easily know which file is modified. So that that we can recover that modified file from specified backup folder.

The second activity performed by user is Process log. In process log activity the server will know which processes are currently running on client machine. In process log activity, server will know which activities are performed by user on client machine. Server send all processes to the client email id. So that client will easily know which activities are performed by client.

II. DATA MINING AND FORENSIC TECHNIQUE

The IIDPS uses data mining and forensic profiling techniques to mine system call patterns (SC-patterns) defined as the longest system call sequence (SC-sequence) that has repeatedly appeared several times in a user's log file for the user. The user's forensic features, defined as an SC-pattern frequently appearing in a user's submitted SC-sequences but rarely being used by other users, are retrieved from the user's computer usage history

III. PROPOSED SYSTEM

Use In this approach, log file is stored into two different forms as well as in two different places. Log file in plain text from is stored on target host and a copy of same log file is stored in another host called log manager. When intruder tried to acquire log file IDS running on the based host to detect exact intrusion and then it will be give an alert to security administrator about the intrusion which is take require decision to mitigate them.

IV. SYSTEM ARCHITECTURE

Fig.1 System architecture

A. Target Host

In the Target Host, Crucial data (i.e. log files) is stored. To preserve the integrity and confidentiality need to be Continuous monitor of log file is prime requirement of the data stored in it. To achieve this, IDS is deployed on target host and it is a continuous process round the clock. Whenever an attacker tries to intrude the target host, IDS running on target host detects the intrusion; sends an alert message to security center as well as log server. After that it will be capture the state of the system (RAM image and log file image) by using Digital Forensic Tool. Then the captured log file has been compared to previous log file image to confirm the intrusion. Target host is nothing but our OS as it was host based system. The intrusion can try to use information of the system but if he try to make changes in the system properties and access the access the records then IDs comes in to the picture.

B. Server

Server maintains the copy of the log file in an encrypted form. Log file maintained the Encryption keys and it kept secret. Periodically back up of the Target host log file is taken and it is stored on the log server. It will be receiving log file as backup and encrypted the file and store within it. Whenever the log server receives an alert message from target host, it decrypts the log file, computes the image of the decrypted log file using digital forensic tool and sends it to the target host to perform the comparison. The main job of the Log server is encryption and decryption of log files such that the intruder doesn't have access to them. If the intruder gets to know the location and condition of the log file shall only be available with the owner and nobody else. It shall be provided at the time of delivering the software as a complete product.

C. Security Centre (Admin)

This is the system used by the security administrator to monitor the alerts generated by IDS. It receives alerts from Target Host. Once the target host has sent the alert to the security Centre , the job of the security Centre starts. The attack is hence detected and looked into at the Security centre. The Security centre is the most essential component of the IDS. Its job is track the intrusion he tries to hack the system, an alert should be sent to the real owner. This will be accomplished by webcam image and same will be prove the again court of law. If the intruder tries to access the files without the net connection, the system shall shut down by itself within 10 seconds, and if he has the net connection intact, then we shall also be able to inform the true owner about the intrusion with the help of an e-mail. In proposed system we are detecting the intrusion through many things like integrity, checking currently running processes, by key log, etc. These all activities are performed by user. The first activity is file integrity. We are detecting intrusion through file integrity. In file integrity concept if any user delete the file or modify file or insert file into specific directory then by Using our system we can detect it. If any file delete or modify of insert into specific folder then that file will save in folder which is specified by client. Then file integrity log send to server. Server sends the integrity of that file to the clients email id. So that client will easily know which file is modified. So that we can recover that modified files from specified backup folder.

V. SYSTEM FRAMEWORK

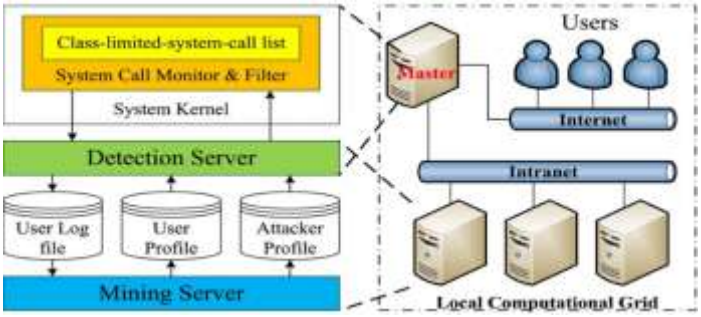

Fig.2 System Framework

In this section, we first introduce the IIDPS framework and describe components of the IIDPS in detail.

A. System Framework

The IIDPS, as shown in Fig. 2, consists of an SC monitor and filter, a mining server, a detection server, a local computational grid, and three repositories, including user log files, user profiles, and an attacker profile.

B. SC Monitor and Filter

An SC in fact is an interface between a user application and services provided by the kernel. Generally, a huge amount of SCs are generated during the execution of a job, i.e., a task or process.

C. Mining Server

As shown in Fig.2 , a mining server extracts SC-sequence generated by a user u from u's log file, counts the times that a specific SC-pattern appears in the file, and stores the result in SC-pattern appearance counts format in u's habit file. After this, SC-patterns' similarity weights are calculated to filter out those SC-patterns commonly used by all or most users. Then, the output result is compared with all other users' habit files in the underlying system to further identify

u's specific SC patterns. Finally, the similarity weight is computed to generate u's user profile.

D. Detection Server

The detection server captures the SCs sent to the kernel by the underlying user u when u is executing shell commands and stores the SCs in the u's log file. After this, the server tries to identify whether u is the underlying account holder or not.

VI. SYSTEM IMPLEMENTATION

Intrusion means someone penetrate the security of the system without permission. Intrusion Detection System (IDS) can detect the illegal activities performed by the Intruders and can report to the higher authorities. IDS is a set of methods and techniques to detect the illegal activities in System level and Network level. IDS can be broadly classified into two, Host Based Intrusion Detection Systems and Network Based Intrusion Detection Systems.

CONCLUSION

In this paper , we bring up an approach to find out user's habit by using data mining and forensic techniques. To identify the representative SC sequences for a user, the frequency that a habitual commands sequence appears in the users log file is counted and its discrimination score is calculated so that users profile can be established . By comparing the users current command with all other profiles ,the IIDPS can identify who the user is. The encryption algorithm is used to provide the security to the files which send over the network and the files which stored in the database. If the user performs some malicious activities then IIDPS will capture the image.

REFERENCES

[1]An internal intrusion detection and protection system using data mining and ACO techniques,

[2] 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.

[3] Q. Chen, S. Abdelwahed, and A. Erradi, ―A model-based approach to self-protection in computing system,‖ in Proc. ACM Cloud Autonomic Comput. Conf., Miami, FL, USA, 2013, pp. 1–10.

[4] 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.

[5] 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.

[6] Z. Shan, X. Wang, T. Chiueh, and X. Meng, ―Safe side effects commitment for OS-level virtualization,‖ in Proc. ACM Int. Conf. Autonomic Comput., Karlsruhe, Germany, 2011, pp. 111–120.

[7] M. K. Rogers and K. Seigfried, ―The future of computer forensics: A needs analysis survey,‖ Comput. Security, vol. 23, no. 1, pp.12–16, Feb. 2004.

[8] J. Choi, C. Choi, B. Ko, D. Choi, and P. Kim, Detecting web based DDoS attack using MapReduce operations in cloud computing environment,‖ J. Internet Serv. Inf. Security, vol. 3, no. 3/4, pp. 28–37, Nov. 2013.

[9] Q. Wang, L. Vu, K. Nahrstedt, and H. Khurana, ―MIS: Malicious nodes identification scheme in network-coding-based peer-topeer streaming,‖ in Proc. IEEE INFOCOM, San Diego, CA, USA, 2010, pp. 1–5.

[10] Z. A. Baig, ―Pattern recognition for detecting distributed node exhaustion attacks in wireless sensor networks,‖ Comput. Commun., vol. 34, no. 3, pp. 468–484, Mar. 2011.

