ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

A Survey on Host Based Intrusion Detection System with Digital Forensics Tools

Varsha Jadhav[1], Archana Mane[2], Ptiyanka Chaudhary[3], Prof. Aparna A. Junnarkar[4]

B. E Student, Department of Computer, P.E. S Modern College of Engineering, Shivajinagar, Pune Maharashtra, India[1]

Assistant Professor, Department of Computer, P.E. S Modern College of Engineering, Shivajinagar, Pune Maharashtra, India[2]

ABSTRACT: In today's technology, new attacks are increase rapidly day by day even though system wrapped within securities then also it will may cause for insecure system. Intrusion detection system these technique help for the find out intrusion in the system. It was primary function of system is detect intrusion and give alerts when user try to intrusion on timely manner. In another word find out intrusion as well as response. When intrusion detect that time IDS unable to provide state of the system. Hence, it fails to preserve the evidences against the attack in original form. New strategy required for maintain reliability and completeness of gathered evidence for later examination hence in these studies we proposed automated digital forensic techniques with IDS. In these technique when IDS find out intrusion it will send alert massage by invoking automated digital forensic tool to the system administrator which is help for the identify state of the system. After these capture image and state of the system used as evidence agains court of law to prove the damage level of the system.

KEYWORDS: EIntrusion Detection Systems, Digital Forensic, Logs, Cryptography.

I. INTRODUCTION

Now a day's Intrusion detection system is most important to safeguard in organization for electronic assets. It was a process of detect traffic in the system and which traffic is harmful for the system, detect which traffic malicious or not by intrusion detection system also monitor and analyse the process of the system. To monitor the traffic which is harmful to the organization policies and standard practices this software or appliance can help effectively. To overcome result risk of the intrusion it continuously watches on the traffic, detect intrusion and give alert in timely manner. IDS broadly classified into two types based on the deployment i.e. Host based Intrusion Detection System (HIDS) and Network based Intrusion Detection System (NIDS) [5]. Host-based Intrusion Detection System as the name implies, it is configured on a particular system/server. Its function is to continuously monitor and analyses the activities only on the system where it is configured. HIDS triggers an alert whenever an intrusion is detected. For instance, alert will be generated when an attacker tries to create/modify/delete key system files. HIDS is work better as compare to NIDS as it was help for analysed incoming encrypted traffic which is not detected by NIDS. NIDS used for detect attacks like Distributed Denial of Service (DDoS) attack, port scan etc. It examines the incoming network traffic to classify as malicious or non-malicious traffic. It was research on payload portion, rearrange the packets and determine if any predefine malicious behaviour was reflected [6]. Recently "Intrusion investigations with data-hiding for computer Log-file Forensics" technique has been proposed [1]. In this approach, log file is stored in two different forms as well as in two different places. There are two form of log file plain form of log file stored on target host and another copy of log file will be stored on log manager and it is hidden in image using steganography. In that case when intrusion try to changes on target host IDS can be running and give alert massage to system administrator. To verify whether the intrusion occurred or not, security administrator use the steno image to extract log file and compares it with log file available in the target host. If the result of the comparison is unequal then intrusion is confirmed else not. Major limitation of this approach is that forensic technique is unable to capture the evidence of the attack. So it is not possible to preserve the log file damage for forensic analysis and evidence cannot be collected immediately against the attack to prove in the court of law. To overcome this limitation, in this work automated Digital Forensic Technique with Intrusion Detection System is proposed. This new technique is crucial requirement because the current IDS are not designed to collect and protect evidence against the attack. Digital forensics plays an important role by providing

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

scientifically proven methods to gather, process, interpret and use digital evidence to bring a decisive description of attack. The objective of digital forensics usage in this work is to explain the current state of system (Target system). Digital forensics technique seeks to capture digital evidence such that the forensic integrity of the data is preserved for legal purposes.

II. RELATED WORK

In "Analyzing multiple logs for forensic evidence", Authors have proposed automatic log analysis technique that is based on computational logic and formal automatic verification [2]. These approaches help for the modeling log events and properties logical presentation which is detect by system events. In log model collect the evidence which is generate by different applications is difficult task for analysts to understand [3]. In proposed approach, authors proposed a system composed by a set of agents to collect, filter and normalize and correlate the events coming from different application log files. It uses both signatures based and anomaly based approach to identify known as well as unknown attacks. It implements log correlation, reinforcement learning and association rule learning collaboratively. It exemplifies the benefits of integrating various artificial intelligence techniques with the Intrusion Detection Systems.

III. PROPOSED SYSTEM

The proposed approach is as shown in Fig. 1. The functions of each entity are described as follows:

- ***Target Host:***

The target host is a system in which crucial data (i.e. log file) is stored. Continuous monitor of log file is prime requirement to preserve the integrity and confidentiality of the data stored in it. To achieve this, IDS is deployed on target host and it is a continuous process round the clock. When attacker tries to make change IDS running on target host and generate alert massage and send I to system administrator, security center as well as log server. After that digital forensic tool can captured the image, state of the system. Original log file image and new captured image can compare and find the intrusion. Result of comparison should be zero if not zero then it will be intrusion.

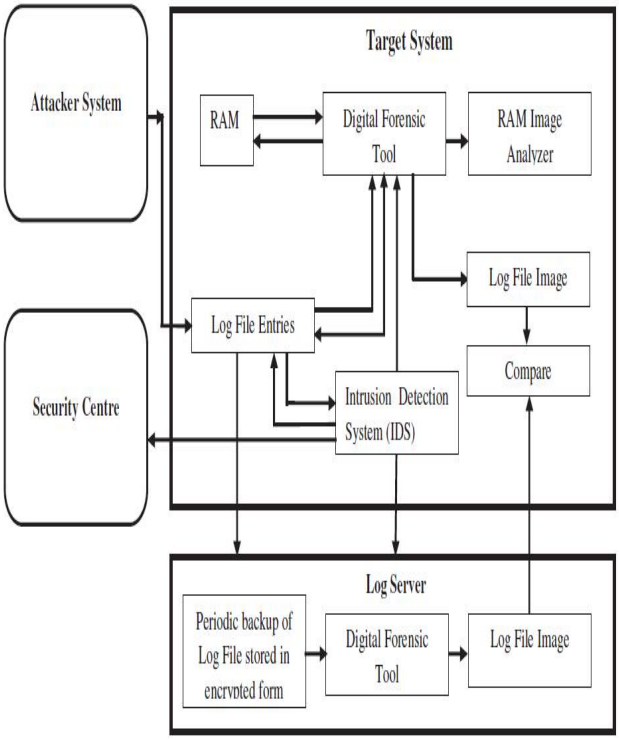

Fig. 1 Automated Digital Forensic Technique with Intrusion Detection System

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

- ***Log Server***

It stores the copy of the log file in an encrypted form. Encryption key maintained only by the log server and it kept secret. Periodically back up of the Target host log file is taken and it is stored on the log server. Upon receiving the log file as a backup, it encrypts the received log file and stores within it. Whenever log server receive a alert message from target host, it decrypts the log file, computes the image of the decrypted log file using digital forensic tool and sends to target host to perform the comparison.

- ***Security Centre***

This is the system used by the security administrator to monitor the alerts generated by IDS. It receives alerts from Target Host. Flow of the entire proposed work is shown in figure 2. This is the system used by the security administrator to monitor the alerts generated by IDS. It receives alerts from Target Host. Flow of the entire proposed work is shown in figure 2.

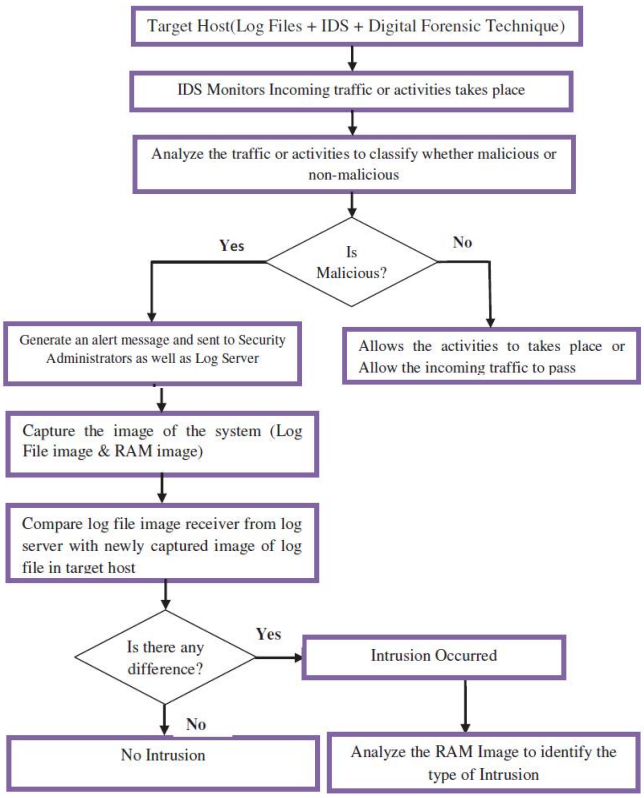

Fig. 2. Flow chart of the proposed work

IV. CONCLUSION

Equalize In this paper for the identify SC pattern for the user we can use data mining and forensic technique. Most commonly used SC-patterns are filtered out when the time that a habitual SC pattern appears in the user's log file is counted, and then a user's profile is established. By identifying a user's SC-patterns as his/her computer usage habits from the user's current input SCs, the IIDPS resists suspected attackers. The experimental results demonstrate that the average detection accuracy is higher than 94% when the decisive rate threshold is 0.9, indicating that the IIDPS can assist system administrators to point out an insider or an attacker in a closed environment. The further study will be done by improving IIDPS's performance and investigating third-party shell commands.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

REFERENCES

1. Ya-Ting Fan1 and Shiuh-JengWang , "Intrusion Investigations with Data-hiding for Computer Log-file Forensics", IEEE 2010.
2. R. Araeteh, M. Debbabi, A. Sakha, and M. Saleh, "Analyzing multiple logs for forensic evidence," Digital Investigation 4S, pp, 82- 91, 2007.
3. J. Herrerias and R. Gomez, "A log correlation model to support the evidence search process in a forensic investigation," Proceedings of the Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'07), pp. 31-42, 2007.
4. BhagyashreeDeokar, AmbarishHazarnis, " Intrusion Detection System using log files and reinforcement learning", International Journal of Computer Applications (0975 – 8887) ,May 2012
5. Karen Scarfone& Peter Mell, National Institute of Standards and Technology (NIST) Special Publication 800-94 , " Guide to Intrusion Detection and Prevention Systems", Feb 2007.
6. Karen Kent, Tim Grance,Hung Dang, NIST Special Publication 800- 86 , "Guide to Integrating Forensic Techniques into Incident Response" , Aug 2006.

BIOGRAPHY

Miss. VarshaJadhav, is Student at Computer Department, P.E. S Modern College of Engineering, Shivajinagar, Pune Maharashtra

Miss. Archana Maneis Student at Computer Department, P.E. S Modern College of Engineering, Shivajinagar, PuneMaharashtra

Miss. Ptiyanka Chaudhary is Student at Computer Department, P.E. S Modern College of Engineering, Shivajinagar, PuneMaharashtra

Prof.Aparna A. Junnarkar is Assistant Professor, Computer Department, P.E. S Modern College of Engineering, Shivajinagar, Pune Maharashtra