www.ijarcsse.com

Volume 2, Issue 1, January 2012 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Review of Computer forensic & Logging System

Mayank Saxena
Department of
Computer Science and Engineering
Patel college of science & Technology
Bhopal,M.P,INDIA

Nikhil kumar singh
Department of
Computer Science and Engineering
Patel college of science & Technology
Bhopal,M.P,INDIA

Satyendra Singh Thakur
Department of
Computer Science and Engineering
Patel college of science & Technology
Bhopal,M.P,INDIA

Parmalik kumar
Department of
Computer Science and Engineering
Patel college of science & Technology
Bhopal,M.P,INDIA

ABSTRACT: Log files helps cyber forensic process in probing and seizing computer, obtaining electronic evidence for criminal investigations and maintaining computer records for the federal rules of evidence. So it can be said that logging is closely related to Forensic Computing. To make the logs admissible for the use in court, there is a necessity to prove that the logs have not been modified after being generated. Moreover, since the logs contain confidential information, they must be protected strictly. Therefore a secure logging scheme that ensures the integrity and confidentiality of the logs is needed. In this paper the log files and their management issue are discussed. The Technical constraint of available log files are identified and presented.

KEYWORDS: Cyber Forensic: Log File

1. INTRODUCTION

Computer forensics is one of the growing concerns in the IT field [1]. Computer forensics is similar to the field of forensics. Analyzer use the science of forensics to hunt a crime scene for evidence of what happened, by whom it happened, and who did what to whom. In the case of computer forensics, the crime scene is the machine that was hacked, the victim is the entity to which the computer belongs, and the hacker is the criminal. The evidence in the case of computer forensics is the trail left by the hacker, which is recorded in the log files. In order for computer forensics to be effective, one must have accurate and trustworthy log files.[2]

In the computer security mechanism, the logs are used to describe the behaviors of the computer system, applications and users, monitoring the user's operations of the system, recording anomalies of the system. Once the system was invaded, we can find out loopholes in the current system by analyzing the logs, identify weak latches in network security, and analyze the possible attacks, and thus take appropriate measures to strengthen the network control.[3] Log data is also an important source of information and should be preserved in digital forensic investigations [4]. To carry out Forensic Computing, trustworthy logs are needed to be admissible for the use in court. Moreover, since the log contains private information, the confidentiality of the log must be preserved. [7]Therefore, the logs' integrity and security are important to the maintenance of the system, monitor on system activity and the security of system[l].

More experienced hackers are aware of log files and will take steps to hide their activities from the network administrator by either deleting the log file altogether or replacing the log file with a copy showing normal network activity. In the first instance, the network administrator will know that an intrusion was detected, but will have no clues as to the identity of the intruder or how the intruder entered the system. In the second instance, the network administrator will have no clues whatsoever, and will have to rely on other methods for detecting intrusion.[2]

2. LOG FILE

Log files are considerable sources for determining the health status of a system and used to capture the events happened within a computer system and networks. Logs are collection of log entries and each entry contains information related to a specific event that has taken place within a system or network. Many logs within an association contain records associated with computer security which are generated by many sources, including operating systems on servers, workstations, networking equipment and other security software's, such as antivirus software, firewalls, intrusion detection and prevention systems and many other applications. Routine log analysis is beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems. Logs are also useful for performing auditing and forensic analysis, supporting internal investigations, establishing baselines, and identifying operational trends and long-term problems [8].

Initially, logs were used for troubleshooting problems, but now days they are used for many functions within most organizations and associations, such as optimizing system and network performance, recording the actions of users, and providing data useful for investigating malicious activity. Logs have evolved to contain information related to many different types of events occurring within networks and systems. Within an organization, many logs contain records related to computer security; common examples of these computer security logs are audit logs that track user authentication attempts and security device logs that record possible attacks.

Log file study a user's query behavior while user navigates a search site. Understanding the user's navigational preferences helps to improve query behavior. In fact, the knowledge of the most likely user access patterns allows service provides to customize and adapt their sites interface for individual users as well as to improve the site's static structure within the wider hypertext system.

Log files helps cyber forensic in probing and seizing computer, obtaining electronic evidence for criminal investigations and maintaining computer records for the federal rules of evidence.

3. LOG FILES IN CYBER FORENSIC

Cyber forensics is the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation and presentation of cyber evidence derived from cyber sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal or helping to anticipate the unauthorized actions shown to be disruptive to planned operations [9].One important Element of cyber forensics is the credibility of the cyber evidence.

In Cyber forensic, log files are like the black box on an airplane that records the events occurred within an organization's system and networks. Logs are composed of log entries that play a very important role in evidence gathering and each entry contains information related to a specific event that has occurred within a system or a network [10].

4. LOG MANAGEMENT

With the world wide deployment of IT field the numbers of threats against networks and systems have greatly increased so revolution of computer security needed variety of computer security logs and their management. Log management is essential to ensure that computer security records are stored in sufficient detail for an appropriate period of time. Log management is the process for generating, transmitting, storing, analyzing, and disposing of computer security log data. The fundamental problem with log management is effectively Log generation and storage, protecting the confidentiality, integrity, and availability of logs.

5. THE CHALLENGES IN LOG MANAGEMENT

In this section we have discussed the mainly common types of challenges, divided into three groups. First, there are several potential problems with the initial generation of logs because of their variety and prevalence. Second, the confidentiality, integrity, and availability of generated logs could be breached inadvertently or intentionally. Finally, the people responsible for performing log analysis are often inadequately prepared and supported.

5.1 Log Generation and Storage

In this section many hosts, operating systems, security software, and other applications generate and store logs. This complicates log management in the following ways:

- Multiple Log Sources – Logs can be found on many hosts throughout the organization that should be required to conduct log management throughout the organization. In addition, a single log source can generate multiple logs for example, an application storing authentication attempts in one log and network activity in another log.

- Heterogeneous Log Content – Log file capture certain pieces of information in each entry, such as client and server IP addresses, ports, date and time etc. For efficiency, log sources often record only the pieces of information that they consider most important. It creates difficulty to make a relationship between event records and different log sources because they may not have any common attribute (e.g., source 1 records the source IP address but not the username, and source 2 records the username but not the source IP address). Even the representation of log value varies with log source; these differences may be slight, such as one date being in YYYYMMDD format and another being in MMDDYYYY format, or they may be much more complex [11,13].

- Inconsistent Timestamps- Usually every application who generates logs uses the local timestamps i.e. the timestamps of the internal clock. If the host's clock is not synchronized or inaccurate, then log file analysis is more difficult, especially when the environment has multiple hosts. For example, timestamps may indicate that event "X" happened 2 minutes after event "Y", whereas event 'X' has actually happened 55 seconds before event "Y".

- Multiple Log Formats- Many of the log source types use different formats for their logs, such as comma-separated or tab-separated text files, databases, syslog, Simple Network Management Protocol (SNMP), Extensible Markup Language (XML), and binary files. Some logs are designed for humans to read, while others are not; some logs use standard formats, while others use proprietary formats. Some logs are created not for local storage in a file, but for transmission to another system for processing; a common example of this is SNMP traps. For some output formats, particularly text files, there are many possibilities for the sequence of the values in each log entry and the delimiters between the values (e.g., comma-separated values, tab-delimited values, XML).

5.2 Log Protection

Because logs contain records of system and network security, they need to be protected from breaches of their confidentiality and integrity. For example, logs might intentionally or inadvertently capture sensitive information such as users' passwords and the content of e-mails. This raises security and privacy concerns involving both the individuals that review the logs and others that might be able to access the logs through authorized or unauthorized means. Logs that are secured improperly in storage or in transit might also be susceptible to intentional and unintentional alteration and destruction. This could cause a variety of impacts, including allowing malicious activities to go unnoticed and manipulating evidence to conceal the identity of a malicious party. For example, many root kits are specifically designed to alter logs to remove any evidence of the root kits' installation or execution [12, 13].

Organizations also need to protect the availability of their logs. Many logs have a maximum size, such as storing the 10,000 most recent events, or keeping 100 megabytes of log data. When the size limit is reached, the log might overwrite old data with new data or stop logging altogether, both of which would cause a loss of log data availability. To meet data retention requirements, organizations might need to keep copies of log files for a longer period of time than the original log sources can support, which necessitates establishing log archival processes. Because of the volume of logs, it might be appropriate in some cases to reduce the logs by filtering out log entries that do not need to be archived. The confidentiality and integrity of the archived logs also need to be protected.

5.3 Log Analysis

In any organization, network and system administrators have traditionally been responsible for performing log analysis studying log entries to identify events of interest. It has often been treated as a low-priority task by administrators and management because other duties of administrators, such as handling operational problems and resolving security vulnerabilities, necessitate rapid responses. Administrators who are responsible for performing log analysis often receive no training on doing it efficiently and effectively, particularly on prioritization. Also, administrators often do not receive tools that are effective at automating much of the analysis process, such as scripts and security software tools (e.g., host-based intrusion detection products, security information and event management software). Many of these tools are particularly helpful in finding patterns that humans cannot easily see, such as correlating entries from multiple logs that relate to the same event. Another problem is that many administrators consider log analysis to be boring and to provide little benefit for the amount of time required. Log analysis is often treated as reactive something to be done after a problem has been identified through other means rather than proactive, to identify ongoing activity and look for signs of impending problems. Traditionally, most logs have not been analyzed in a real-time or near real time manner. Without sound processes for analyzing logs, the value of the logs is significantly reduced [12].

6. LOG MANAGEMENT INFRASTRUCTURE

A log management infrastructure consists of the hardware, software, networks, and media used to generate, transmit, store, analyze, and dispose of log data. Most organizations have one or more log management infrastructures [12,13].Infrastructure typically comprises the following three tiers as show in figure 1:

6.1 Log Generation- The first tier contains the hosts that generate the log data. Some hosts run logging client applications or services that make their log data available through networks to log servers in the second tier. Other hosts make their logs available through other means, such as allowing the servers to authenticate to them and retrieve copies of the log files.

6.2 Log Analysis and Storage- The second tier is composed of one or more log servers that receive log data or copies of log data from the hosts in the first tier. The data is transferred to the servers either in a real-time or near-real-time manner, or in occasional batches based on a schedule or the amount of log data waiting to be transferred. Servers that receive log data from multiple log generators are sometimes called collectors or aggregators. Log data may be stored on the log servers themselves or on separate database servers.

6.3 Log Monitoring- The third tier contains consoles that may be used to monitor and review log data and the results of automated analysis. Log monitoring consoles can also be used to generate reports. In some log management infrastructures, consoles can also be used to provide management for the log servers and clients. Also, console user privileges sometimes can be limited to only the necessary functions and data sources for each user.

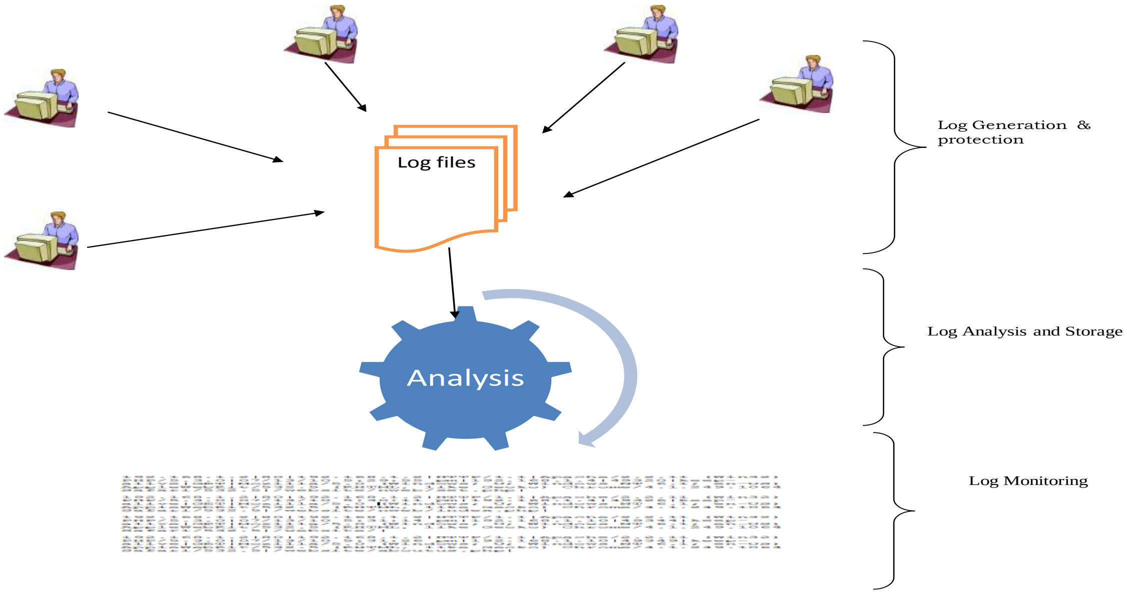

Fig1: Log Management Infrastructure

7. CONCLUSIONS

Log file are mostly captured the behavior of machine not the behavior of end user. Log file provide troubleshooting, security and pro-active system administration that provide significant help in caching suspicious end user and in process of cyber forensic. Moreover, since the logs contain confidential information, they must be protected strictly. Therefore a secure logging scheme that ensures the integrity and confidentiality of the logs is needed.

8. ACKNOWLEDGMENTS

The research presented in this paper would not have been possible without our college, at PCST, Bhopal. We wish to express our gratitude to all the people who helped turn the World-Wide Web into the useful and popular distributed hypertext. We also wish to thank the anonymous reviewers for their valuable suggestions

References:

[1] Kessler, M. G. (2006). Kessler’s Corner: The growing field of computer forensics. The Kessler Report, 9(1), 7.

[2] Bernie Lantz,Rob Hall, Jason Couraud, “Locking Down Log Files: Enhancing Network Security By Protecting Log Files” Issues in Information Systems Volume VII, No. 2, 2006

[3] ZhiyongWu , Bin ZhuGe Weiming Wang ,”Tamper Resistance Protection Of Logs Based On Forward-Secure” Institute of Network and Communication Engineering, Zhejiang Gongshang University , 2010 IEEE

[4] L. Volonino, “Electronic evidence and computer forensics,”Communications of the Association for Information Systems,vol. 12, Article 27, 2003.

[5] E. Casey, “Error, uncertainty and loss in digital evidence,”IJDE, vol. 1, no. 2, 2002.

[6] Benjamin Boeck, David Huemer, A Min Tjoa,Towards more Trustable Log Files for Digital Forensics by Means of “Trusted Computing” in 24th IEEE International Conference on Advanced Information Networking and Applications, 2010

[7] Nobutaka Kawaguchi, Shintaro Ueda, Naohiro Obata, Reina Miya ji, Shinichiro Kaneko, Hiroshi Shigeno, Kenichi Okada,” A Secure Logging Scheme for Forensic Computing” Proceedings of the 2004 IEEE Workshop on Infonnation Assurance United States Military Academy , West Point, NY 10-11 June

[8] Muhammad Kamran Ahmed, Mukhtar Hussain and Asad Raza “An Automated User Transparent Approach to log Web URLs for Forensic Analysis” Fifth

International Conference on IT Security Incident Management and IT Forensics 2009.

[9] http://www.cyberforensics.com

[10] Pavel Gladyshev “Formalising Event Reconstruction in Digital Investigations” Ph.D. dissertation Department of Computer Science, University College Dublin, 2004.

[11] Carrier, B.D., Spafford, E.H “Defining Digital Crime Scene Event Reconstruction” Journal of Forensic Sciences, 49(6). Paper ID JFS2004127,2004

[12] Stevens, M.W. “Unification of relative time frames for digital forensics”, Digital Investigation journal, 1(3), pp. 255-239, 2004

[13] Karen Kent and Murugiah Souppaya, “Guide to Computer Security Log Management”, Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, 2006