The Role of Audit Logs in Cyber Security

1 P. K. Sahoo
1Professor, Department of Computer Science and Engineering, Visvesvaraya College of Engineering and Technology
Ibrahimpatnam, Hyderabad-500005, (AP), India.
Email - s_pks@yahoo.com

2 Dr. R. K. Chottaray
2Professor, Department of Computer Science and Engineering
NIT Rourkela, Orissa-769008, India
Email – rkc_ray@rediffmail.com

Abstract: Now a day’s Viruses, Worm attacks, Denial of Service attacks and NetBIOS attacks becoming the head line topics in many new channels. The Internet is becoming one of the critical infrastructures for individuals and corporations to carry out critical business processes have provided a playing field for intruders to carry out different attacks on the network and the system. Every day there are reports of loss of critical data, cyber attacks, hacking of systems and web sites etc. In this scenario log data are very useful as it contain information related to types of events/attacks occurring within the networks and host systems. Log data are very useful to track the history of an intruder’s activity in day-to-day work and providing evidence to investigate malicious activity. Hence log files, which are most significant for cyber security investigation, should be stored in a secured place so that intruders could not able to alter or erase log files. Windows operating systems produce audit log data that are written to the event log in a binary format but windows event log has many limitations. One of the limitations of windows operating system event log is that, it is incapable of handling of messages form network devices such as routers and switches. The proposed architecture is very efficient to capture log data from anywhere in the networks. The solution proposed here greatly simplifies the process of log analysis by centralizing the logging process from all the devices present in the network and also provide a secured storage for the log data. The proposed system also makes it possible the event log of Windows operating system to be compatible with the logging function of other operating system.

Keywords: Cyber attacks, Syslog, Log management.

1. INTRODUCTION

There are continuous reports of Internet security problems due to the increased dependency over the Internet by organizations and individuals to carry out critical business processes. As society grows increasingly dependent on the Internet for commerce, banking, and mission-critical applications, the ability to detect and neutralize network attacks is becoming increasingly significant [1]. The number of cyber attacks increased by 93 percent from 2009 to 2010, reports security vendor Symantec. The company said 286 million new threats were reported last year, including attacks on corporate systems and those that occurred via social networks [2]. Breaches of personally identifiable information have increased dramatically over the past few years and have resulted in the loss of millions of records, which creates a serious security problem both for the individuals and organizations [3]. Security and privacy become great concern for this new world. To meet this challenge, Cyber Trust Program at National Science Foundation has adjusted its research funding directions [4]. Current Web browsers are plagued with vulnerabilities, providing hackers with easy access to computer systems via browser-based attacks [5]. Computer and network attacks are the product of an attackers understanding of the strengths and weaknesses in the operating systems, features of popular software, networking protocols and programming languages [6]. In the recent development stated above, security log data are very useful as security device logs that trace possible attacks from the attackers and record the day-to-day activity of system users. In recent years, it has become important for researchers, security incident responders and educators to share network logs and many log tools and techniques have been developed to sanitize this sensitive data source in order to enable more collaboration. Unfortunately, many more attacks have been created, in parallel that try to exploit weakness in the process [7]. In most of companies or organizations, logs play important role in information security [8]. Logs are one of the most fundamental resources to any security professional. It is widely recognized by the government and industry that it is both beneficial and desirable to share logs for the purpose of
security research [9]. Today log traces are widely used to identify and prevent violations of corporate information systems [10]. It is important to maintain Internet security system during and after the occurrences to collect evidence and forensics essences by various devices, such as hard disks, system logs, firewall, IDS log, processes as well as Internet connections [11]. Now many of the significant worms are designed to steal sensitive information such as pin codes, social security numbers, credit card numbers and passwords, from which the attacker can capture the information for hacking the network. Even encrypted web transactions may not protect sensitive information. Hence administrators should not only rely on Anti-Virus software and email filtering to detect worm infections. Logs from firewalls, intrusion detection systems and proxy server logs should be monitored periodically to protect from infections [12]. After analyzing the requirements of log service on large scale information management system, the idea of specialization, high reliability, easy to operate and management of logs comes out to sort out the problems of limitation of current log management system [13]. The intruders are able to conceal their attacks by disabling logging facilities or modifying the log files so that their activity goes unnoticed. When an intruder is trying to enter into the network, the first thing, he or she probably do is completely remove log files, or wipe out evidence of his trespass out of those files. Hence log management is essential to ensure that computer security records are stored in sufficient detail for an appropriate period of time. Computer security breaches are already a major problem. The most basic defense against it is to monitor and audit the computer logs. It is impossible to inspect them by using the current systems [14].

Operating system logs and application logs are an untapped mine of vital information about the strength and safety of organization’s computer infrastructure. Originally logs were mainly used for troubleshooting problems but now logs serve many functions within most organizations, such as optimizing systems 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 the networks and systems. For example audit logs that track user authentication attempts and security device logs that record possible attacks from the attackers. When properly configured, these logs record the day-to-day activity of system users; administrative changes made by folks who manage critical production systems; and capture evidence produced by malicious activity. With the right logging configuration we will able to capture the history of a hacker’s activity on our computer system, from the establishment of unauthorized accounts to the installation of back-doors, enabling us to quickly isolate and repair affected systems after an intrusion [15-21]. Hence log data is most vital to deal with the cyber security problem but it is a challenging task.

2.1. THE NEED FOR LOG MANAGEMENT

The number, volume and variety of computer security logs have increased greatly, which has created the need for computer security log management. The log management refers to the process for generating, transmitting, storing, analyzing and disposing of computer security logs. Log management is essential to ensure that the computer security records are stored in sufficient detail for an appropriate period of time. Routine log analysis is beneficial for identifying security incidents, policy violations and operational problems. Log data are also very useful when performing auditing and forensic analysis, supporting internal investigations, establishing baselines, identifying operational trends and long-term problems. Log management also involves protecting the confidentiality, integrity and availability of log files.

2.2. THE CHALLENGES IN LOG MANAGEMENT

A fundamental problem with log management that occurs in many organizations is effectively balancing a limited quantity of log management resources with a continuous supply of log data. Log generation and storage can be complicated by several factors, including a high number of log resources, inconsistent log content and time stamps among sources. Some of the difficulties in log management are as below.

- Many Log Sources

Logs are located on many hosts throughout the organization, necessitating log management to be performed throughout the organization. Also a
single source can generate multiple logs. As example Intrusion detection system record detail information on suspicious behavior and detected attacks, anti-malware software records all instances of detected malware and system disinfection attempts.

- **Inconsistent Log Content**

Each log source records contain information in its log entries, such as host IP addresses and usernames. For efficiency, log sources often record only the pieces of information that they consider most important. This makes it difficult to link events recorded by different log sources because they may not have any common values recorded.

- **Inconsistent Timestamps.**

Each host that generates logs typically references its internal clock when setting a timestamp for each log entry. If a host’s clock is inaccurate, the timestamps in its logs will also be inaccurate. Time stamp are required to indicate the sequence of events during log analysis.

### 2.3 KEY PRACTICES IN LOG MANAGEMENT

Most of the organizations recommended the following key practices to meet the challenges in Log management.

- Prioritize log management appropriately throughout the organization.
- Establish policies and procedures for log management.
- Create and maintain a secure log management infrastructure.
- Provide proper training for all staff working in log management.

**Log Management Infrastructure**

A log management infrastructure consists of hardware, software, networks and media used to generate, transmit, store, analyze and dispose of log data. Log management infrastructure typically performs several functions that support the analysis and security of log data. A log management infrastructure typically consists of the following three tires.

- **Log Generation.** The first tier contains the hosts that generate the log data. Most organizations use several types of network-based security software to detect malicious activity. Accordingly security software is a major source of computer security log data. The most common form of antimalware software is antivirus software, which typically records all instances of detected malware, file and system disinfection attempts and file quarantines.

- **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. Log data may be stored on the server themselves or separate database servers.

- **Log Monitoring.** The third tier contains consoles that may be used to monitor and review log data and 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.

### 2.4 LOG MANAGEMENT IN WINDOWS ENVIRONMENT

Windows operating systems (Windows NT, 2000, XP) and applications produce audit data that are written to the windows event log in a binary format. The event log data can be examined by the windows event viewer application. The event log allows log records to be collected for display and altering. It also specifies events based on event log file, event ID, event source and of event type. Events collected from the Event logs can be consolidated into longitude event, which makes them readily available for evaluation, analysis; display and reporting. Event log reports shows statistics related to a number of event log records of each type. One of the limitations of windows event log is because of it’s distributed in nature and there are no native windows tools available to facilitate the centralization of logging process. Each event log resides locally in the host system.
and centralization of log files is not possible, which makes log management most difficult. UNIX operating systems comply with the Syslog specification whereas windows do not comply with the syslog specification. Hence a separate tool or application program is required to translate event log binary format to syslog message format.

2.5 LOG MANAGEMENT IN LINUX ENVIRONMENT

Linux operating systems (UNIX, Linux, and Sun Solaris) and applications produce audit data that are written to the Syslog in a plain text format. All UNIX based operating systems have Syslog implementation, which allows the centralized collection of log files from network devices, workstations and servers.

3. PROPOSED SYSTEM.

3.1 SYSTEM DESIGN

The diagram given below (Fig. 1) is the structural model of the proposed system architecture. The log files store information related to type of events/attacks occur in the network and record the sequence of user’s action, which is very useful for investigation. The centralization of log data greatly simplifies the log management process. The system proposed helps in a great way to centralize the storage and interpretation of logs of an organization. The architecture proposed consist of various sub-systems such as Sniffer sub-system, Unix host sub-system, Router and Firewall sub-system, Windows host sub-system, Event collector sub-system, Winsyslog server sub-system, Encryption sub-system and Storage sub-system. The Sniffer Sub-System captures the packets form the network. The Sniffer sub-system can be easily implemented using jpcap. The packets are captured using the class jpcapCaptor. The UNIX host sub-system write log data in Syslog format. The Windows host sub-system generates log data that write to event log. As the log data in the event log of Windows host sub-system is in binary format, the translator receives the log data from the windows native event log in binary form and translates it into Syslog message format. The event collector sub-system is to collect the log data from the UNIX host, Sniffer Sub-System, Router and also from other hosts. As windows do not comply with the Syslog specifications, we proposed to implement the translator by using some of the available free tools such as Event Reporter or Kiwi Syslog daemon, which can be used to access event logs in windows network. This makes it possible the event log of Windows host sub-system to be compatible with the logging function of other operating system. The event collector then sends the collected log files to the WinSyslog Server for further processing. The encryptor sub-system then encrypted the log files by using a very strong encryption technique before sending it to the central storage. Centralization of the log data serves to protect critical audit data from the attackers by removing it immediately from the host, on which it is generated. The central storage provides a secure and forensically sound storage of the log data, where it is difficult for an intruder to alter or erase the log files.

3.2 ARCHITECTURE
3.3 ADVANTAGES OF THE PROPOSED SYSTEM

- Events which are collected at the Event collector sub-system can be easily coordinate and warrant can be sent out to interested parties as warranted.

- Log data remain on the central storage for a period of time, even if the sending system fails or the logs on it are accidentally erased.

- Access to all the events or logs can be provided through a central interface.

- The central storage provides a secure and forensically sound storage of the logs, where it is far difficult for an attacker to alter or destroy log files.

- Centralized logging process using the Syslog protocol allows the Event collector to collect log files from almost all log generating devices present within the network, thus greatly simplify the process of analysis.

4. CONCLUSION

Security-related threats are becoming disrupting and more damaging day by day and becoming the headlines for news papers and magazines. As the internet grows due to the increasing demand by organizations and individuals, the attackers are taking advantages of the vulnerabilities of the
network and are easily accessing the system and the network by altering or erasing the log data. Log data are very useful for any organization as it used to track the activity of the intruder and also providing useful data for investigating malicious activity. Hence log management is required as a helping hand to cyber security by protecting the log files from the attackers, who are trying to alter/erase the log files in order to wipe out evidence of his trespass out of those files. The proposed architecture is very efficient to centralize the storage and interpretation of log data of an organization and greatly simplifies the log management process. The limitations of the distributed nature of event log service in windows can be easily overcome in the proposed solution and also makes it possible to be compatibly with the logging function of the other operating systems. The architecture can be easily extended in the future for other devices also. The proposed work also offers stronger security capabilities such as reliable log delivery; provide secure and forensically sound storage of the log data and also simplify the process of log analysis.

5. REFERENCES


