Research and system Design and Implementation of Computer Forensics Based on Log

Xiaobo Ming
{ mingxiaobo@126.com}

Shangrao Vocational Technical College Shangrao 334109, Jiangxi, China

Abstract. Log is an important document produced and retained by the computer system, it records a large number of criminals using computers to commit crimes, is a very important source of clues and evidence against computer crime. To well using log to implement computer forensics, there are two problems that need to be solved: one is in a timely manner to the log system protection, in accordance with the procedure of computer forensics to extract the log; second is how to log analysis, find out the crime of "traces", as a valid evidence demonstrating to the court. In this paper, combined with the domestic and foreign experience in the fight against computer crime, the process and steps of computer forensics technology are discussed. And existing problem in this thesis, the status of the computer forensics technology and research of log, analyzes the computer systems of all kinds of log files and format, proposed a relatively perfect supporting computer forensics security audit log method, and according to our current level of technology, design a more suitable for law enforcement agencies in the application of the computer log forensics system.

Keywords: Log file; computer forensics; electronic evidence; computer crime; security audit.

1 Introduction

In recent years, the rapid development of China's information technology and information industry, computer technology especially Internet on China's politics, economy, military, science and technology, culture, education, health, and the people's daily life and so on national economic and social development in various fields have widely provides a new crime means and far-reaching impact, but also for the criminals. Development trend of increasingly serious presented a computer crime (ComPutercirme), from the original only for money crime, for the development of the crimes in multiple areas of political, military, and intellectual property rights; from the unit crime, development to today's cyber crime, information crime. Computer crime has caused serious threats to national security and social stability, which has seriously harmed our country's political security, economic security and social stability [1]. Computer crime is a criminal offense in a new high-tech crime, procuratorial, judicial and public security organs in how to use high-tech means against the high technology crime aspects lack of necessary technical support and guarantee, seriously affected the efforts to combat computer crime activities. In order to promote what is beneficial and abolish what is harmful, maintenance of social and political stability in China, security and promote the

healthy and orderly development of the computer information network, ability to improve the judicial authorities to crack down on the use of computer technology that endanger network security and information security and other types of crime, already no time to delay. System in the log (Log) records of the use of computer criminals to commit a large number of computer crimes, as the fight against computer crime is very important clues and evidence. But computer system generated log files basically without protection mechanism, easy to be an intruder to modify, delete or forged, the computer system log as the electronic evidence (lEectroincEvidecne) often received the court questioned. To the existence of various systems in the log file of security audit, collection, conservation, analysis and archiving, to ensure that the log file complete and true to the log file as effective evidence presented to the court, has become an urgent need to study the problem. Computer log forensic technology is one of the main means to solve these problems, and become the basic work of all companies and government departments to ensure information security, play a very important role in the fight against computer crime. Log files are generated by the computer system running the internal program, almost every system has its own log files. Log records the day-to-day running of the system, through which to examine the error occurred, or look up when attacked by attackers left "traces", it can real-time monitoring system, monitoring and tracking intruders and so on. The role of the log for the security of the system is obvious, whether it is a network administrator or hackers are attached great importance to the log. An experienced administrator can quickly learn the security performance of the system, and a smart hacker will often quickly cleared away after the invasion of the invasion of their own bad log. At present, a variety of operating systems and application software itself has a lot of loopholes, the system log is not very good protection mechanism, so that the log file security risks exist [2].

2 System Related Technology Analysis

The commonly used by hackers attack techniques mainly include: password attacks, buffer overflow attacks, port scans, deception attack, network monitoring, placed a Trojan horse, denial of service (DOS) attacks and distributed denial of service (DDoS) attacks. The current commonly used network security tools include: network isolation, port scanning, firewall, intrusion detection system (IDs) and virtual private network (VPN), etc.. These tools can protect the network from different aspects, but they are from the point of view of the prevention of the invasion. Because of the increasing use of these tools, the use of these tools does not guarantee that the network will not be invaded. For example, there have been some ways to bypass the firewall and the failure of the intrusion detection system. Once the network has been invaded, and caused a loss, of course, would like to resort to the law to protect their rights and interests and to obtain compensation, and therefore the computer forensics becomes very important. Computer forensics? That the article published in the IEEESecuriyt LeeGarber, computer forensics is analysis of hard disk drive, CD, floppy disk, iZp and jazz in the disk, memory buffers and other forms of storage medium to find evidence of a crime. UdJdoRbbins, a senior expert on computer forensics, gives the following definition: computer forensics is the use of computer research and analysis techniques to identify and extract potential, legally effective evidence. Computer emergency response group and NeweTchnologies certification consulting company further expanded the definition: Computer Forensics includes the protection of computer evidence code information to magnetic media

storage, recognition, extraction and archiving. Management and audit system and network security association sans are attributed to: computer forensics is to use software and tools. According to some pre-defined procedures, comprehensive check computer system, to extract and protection of computer crime evidence [3].

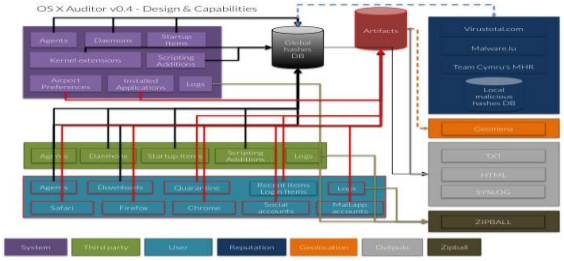

Fig. 1. Schematic diagram of Computer Forensics

2.1 Electronic Evidence

Computer forensics is mainly about electronic evidence to work, the purpose is to make the information stored in the computer and related equipment to reflect the crime of criminal evidence provided to the court. Electronic evidence, also known as computer evidence, refers to the electromagnetic records that are generated during the operation of a computer or computer system, in which the contents of the records are recorded to demonstrate the facts of the case. Electronic evidence on the computer screen performance is a variety of forms, especially the emergence of multimedia technology, electronic evidence combines text, graphics, images, animation, audio and video information of various media, which exists in the form of multimedia computer evidence covers almost all the traditional types of evidence. As with traditional evidence, electronic evidence must be: credible, accurate, complete, and consistent with the laws and regulations, which can be accepted by the court. Electronic evidence is mainly from two aspects, one is the system, the other is the network. From the system of electronic evidence include: system log, audit records system, operating system and database of temporary files or hidden file, database operation record and exchange of hard disk drives swaP partition, sector gap (slack) and free zone, software settings and, to complete the specific features of the script file, web browser data buffer, bookmarks, history, or log sessions, ARP cache, kernel statistics, data memory, physical configuration, network topology and generated by the application software record and log. Evidence from the network firewall log, dis log, the router logs, FTP, WWW and e-mail service log, Emall raw data, real-time chat, network traffic monitoring and other online tools record and log etc.

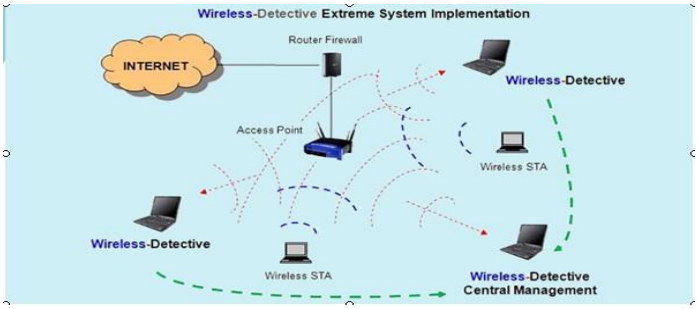

Fig. 2. Schematic diagram of electronic evidence

2.2 Trap Technology

If there is no enough of the electronic evidence, investigators can by trap technique to obtain the suspect records: trick each access to a controlled server to obtain relevant information; by setting hoenyPot (honeypot) hacker deception is set some obvious loopholes in the server hacker deception attack, and record all the intrusion record 26 using specific intrusion detection system. Commonly used in electronic evidence collection techniques include: the security of computer system and file access to: avoid any damage and disruption of the original medium; technology for data and software security gathering; safety on disk or other storage medium without damage mirrored backup technology; already deleted file recovery and reconstruction technology; to exchange files, the information contained in the cache files, temporary files recovery technology; computer in memory of the activity at a particular instant of time data collection technology; network flow data access technology. In the process of electronic evidence collection, will be collected data from the target machine safely transferred to forensics equipment will inevitably need to secure transmission technology, using RS 232 interface transmission cable for asynchronous transmission, to ensure that the whole process of computer forensics has do not tamper with nature. Secure transmission technology mainly uses encryption technology, such as encryption, vPN tunnel encryption, SSL encryption protocol standard, to ensure the safety of data transmission. In addition, by using the message authentication code (MA) C to ensure the integrity of the data in the transmission process [4].

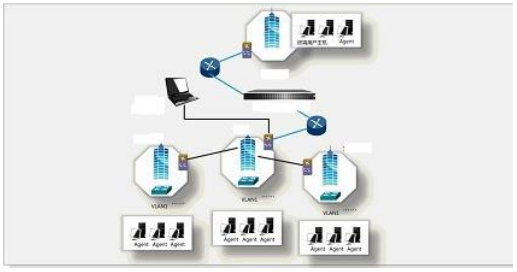

Fig. 3. Schematic diagram of trap technique

2.3 Analysis of Electronic Evidence

The analysis of the electronic evidence and the result report is whether the electronic evidence can be displayed in court, as an important process of the criminal evidence of computer crime. Analysis involves the use of a series of keyword search to obtain the most important information; on file attributes, file digital abstract and log analysis; analysis iwndows exchange files, document fragments and unallocated space data; the electronic evidence do some intelligent correlation analysis, namely: To explore the links between different evidence of the same event. After the completion of the analysis of the electronic evidence the proof of experts give, the ordinary criminal investigation when forensic role similar. To involve the computer crime and the date and time, the hard disk partition, operating system and version, running the forensics tool data and operating system integrity, computer virus assessment, file type, the software license and forensic experts on electronic

evidence analysis and evaluation report, etc. file form can be provided to the court of the electronic evidence.

3 Design and Implementation of the System

Due to the different operating systems, application software, network equipment and services in the network to produce a different log files, even if the same services such as 115 can also be used in different format log file log information. At present, the international community has not yet formed the standard format of the log and the system developers and network equipment manufacturers often according to their own needs develop own log format, the different system log format and stored differently. How to get all kinds of different log files from different systems as the electronic evidence against computer crime becomes particularly difficult. A system log is on this system is involved in the operation of information according to the time sequence as a simple record, only reflect certain events of the system operation, does not fully reflect the to the activities of the situation of a user. A user in the process of network activity will leave traces in the system log many, such as firewall log, IDS logs, operating system log, between these different log exists a causal link to reflect the user's activities. Only the log of multiple systems analysis, can accurately reflect the user's activities [5].

4 Conclusion

With the development of computer technology and the popularization of information technology, all kinds of computer crime is becoming more and more serious. How to carry on the computer forensics, obtain the electronic evidence related to computer crime, the computer criminals to justice, become a major problem to be solved in the judicial department. Unlike traditional forensic analysis, as far as possible from the evidence in the sample to obtain more information, the computer forensics analysis is from massive and real-time data to obtain evidence information, making the computer forensics technology is more complex. In dealing with the actual computer crime cases, but also the lack of standards and protocols for computer forensics, a lack of effective tools for evidence collection.

References

[1] Yu Li. Computer forensics and its standard discussion on. computers and Telecommunications. No. 03. (2016).

[2]. Wang Lu. Research of. network security technology and application of computer forensics experiment teaching. No. 01. (2014)

[3] Wang Lu. Research and discussion of. information network security construction of computer forensics laboratory. No. 07. (2013)

[4] door fly, Jiang Xin, Chen Kangkang. Research and design of computer forensic system. digital technology and application. No. 08. (2013)

[5] Li Junli, Song Lei. Computer forensics in the cloud computing environment. Henan science and technology. No. 01. (2011)