Design and Implementation of Network Forensic System Based on Intrusion Detection analysis

JIANG Liu
Department of Information Engineering
Shenyang Institute of Engineering
Shenyang , China
E-mail: ellenjiang2006@yahoo.com.cn

TIAN Guiyan
Department of Calculating Center
Shenyang Institute of Engineering
Shenyang , China
E-mail: bstgy@sohu.com

ZHU Shidong
Department of Information Engineering
Shenyang Institute of Engineering
Shenyang , China
E-mail: zhusd519@163.com

***Abstract*—To meet the needs of the digital evidence on legal action proceedings, network forensics technology plays an important role in the process of fighting against computer crime and hacking crime. To try to solve some problems of eliminating intrusion track after hacking and some drawbacks of network forensics products, in this paper, we present a network forensic solution which adopts dynamic and static methods to analyze network intrusion data and make detailed records of the data and log. This network forensics solution is able to carry out deep and multi-angle forensic analysis with network evidence, and can ensure the reliability and credibility of the network evidence through effective technical methods.**

Keywords- Digital Forensics; Network Forensic; Forensic analysis; intrusion analysis.

I. INTRODUCTION

With the development of information technology, computer and network have become the indispensible tools of business operations in social life. The popularity of computer and network makes network-based criminal phenomena to occur constantly, and has a growing trend. Nowadays, internet hack attacks have become increasingly rampant, and hacker's technical means are also increasingly complicated. Many government departments, research institutions, military departments and key enterprises etc. have become the main target of hacker attack, hackers' illegal conduct have caused irreparable disaster and wastage to society and business. To combat computer crime, deter Internet fraud and hunt down the criminals of the computer business, digital evidence relying on computer and network plays an increasingly important role in the process of providing evidence of crime, and it has been becoming one of the new evidence modes in litigation process.

The forensics case need to extract data from computer systems and network, or even need to re-obtain information from the files that have been deleted, encrypted or damaged, this form of accessing evidence is called computer and network forensics[1]. The term of network forensics generally refers to the process of getting digital evidence by network event recording and analyzing[2]. Compared with computer forensics, network forensics is more focused on network intrusion and attacks analysis, and collection evidence using network packets and other technical mediums. Network forensics is usually used in conjunction with the network defense technologies, such as network quarantine, firewall, intrusion detection, vulnerability scan, virtual private network.

There are some major problems faced by network forensics—include the difficulty of data collection and analysis caused by mass data, the lack of standards processes of evidence collection, the poor network safety consciousness, etc. Moreover, network forensics products on the market also have the drawbacks of lack of log collection, inaccuracy time, unreasonable forensic analysis, etc. To solve the problems above, we proposed a network forensic system which includes network evidence capturing and network evidence analysis process, this system uses effective technology tools to enhance the reliability and credibility of network evidence, and is able to deeply analyze network evidence in multi-angle.

II. CHARACTERISTIC OF HACKING

The hacking process generally involves the following steps: Firstly, make a footprinting—to determine the target host or server that will be attacked, and analyze them. Secondly, to try to capture the network information of the target host through various methods of network scanning. Then the next step is to commit intrusion to the host system and to get the operating authority using the system's vulnerability. Next, leave a backdoor in the target host for re-entering the system in the future. Finally, the invaders will usually eliminate the system log, delete copied files using specialized tools to hide the traces of their invasion and clear away evidence.

III. DESIGN AND IMPLEMENTATION OF NETWORK FORENSICS SYSTEM

A. System Architecture

The main functions of network forensics system are to record the behavior of intruders, and provide a forensic tool to

978-0-7695-4881-4/12 $26.00 © 2012 IEEE
DOI 10.1109/ICCECT.2012.51

analyze these records, so that the information of intruders and the invasion process will be found out clearly. Network forensics system usually consists of the host that will be checked, the network forensics device and network forensics analysis device. The host that will be checked is usually equipped with software modules to collect system information, and sent the log messages to the network forensics device; the main task of network forensics device is to capture and store the forensic data which include networkstream and log messages from the host that will be checked. The network forensics analysis computer will analyze the capturing data and provide the analysis record of the result.

"Fig. 1" showed the architecture of the network forensics system which includes two engines: the network evidence capturing engine and the network forensic analysis engine. The network evidence capturing engine is used to obtain network evidence, including the network data stream and log messages. According to the different sources of evidence, it can be divided into network data acquisition engine and log message capturing engine. The network forensic analysis engine is used to analyze network evidence, and gives forensic analysis records.

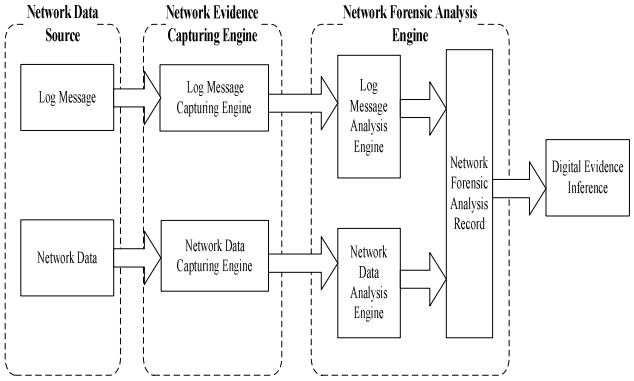

Figure 1. Network Forensic System Architecture

B. *Design and Implementation of Network Data Capturing Engine*

There are two important sources of network evidence--the system logs and network data stream. The network evidence capturing engine is able to obtain the data that access the being forensic host and store these data in accordance with certain storage solutions. These network data are the source of forensic analysis in the future, and is also the important original evidence.

The network data are captured by packet capture device and are stored to files according to the original format of packets, these files are called network data files[3]. The files which include the data of fixed time part will be stored to disk by a time segment, and named after the start time and end time. Firstly, the network capturing engine will set NIC to promiscuous mode, so that it can monitor the being forensics host. Then it start to receive every packet, read its head information, and match them with the corresponding rules. If the conditions are met for capturing, the packet will be stored to the network data file, or it will be discarded. In order to ensure the integrity of the network data files, we utilize MD5 algorithm to sign the network data file, so that we can find out whether the file has been modified throughout MD5 checksums in the process of network forensic analysis.

The network evidence capturing engine need to read a large number of network packets, this process mode will lead to system overhead expensiveness. Firstly, to avoid this problem, we send network packets directly to the system predistribution address space using DMA mode, and at same time, map the memory area that store data packet in system kernel to application program space, so that the network evidence capturing engine can access this memory directly, we can reduce the memory copy action from system kernel to user's space. Secondly, a kernel cache will be allocated in the process of NIC driver module startup, at same time a data structure will be build for management, so the data packet from NIC will be written to the cache directly using DMA. At end, the cache address will be transmitted to user process through proc file, user process will get this address from proc file and make address mapping to read the data.

C. *Design and Implementation of Log Message Capturing Engine*

Log message capturing engine needs to quickly transfer the forensics system log data to forensic device for preventing hacker to delete it. The log information is documented the events in detail that occurred in the system, these logs should be stored to network forensic device in accordance with a certain amount of storage solutions, for they are the sources of forensic analysis, and are also the important original evidence.

The process of log capturing is performed by log sending Agent in host that will be checked and log receiving Agent in forensic device. Firstly, the log sending Agent will read parameters from configuration file and sent them to log receiving agent which will then store them to log files, and make MD5 signature through which the files will be found out modification or not. The communication protocol between the log sending Agent and log receiving Agent is TCP protocol, and use the SSL protocol for encryption and authentication. The SSL protocol which can perform the encryption and authentication of data transmitted is a security protocol between TCP layer and application layer.

D. *Design and Implementation of Network Forensic Analysis Engine*

Network intrusion analysis is referred to analyze network data files using off-line intrusion detection method to analyze the network data files and to find out the invasion and intrusion process[4]. There are two ways for network intrusion analysis: pattern matching and protocol analysis. Pattern matching method which is attack signature-based network intrusion analysis techniques will compare the network packets in the network data files with known intrusion feature library to find out the intrusion behavior against security policy. The principle of the protocol analysis is to identify the packet's protocol type, and use appropriate data analysis procedures to analyze the packets[5]. All protocol can be regarded as a protocol tree, and a

particular protocol will be a node of the tree, a network packet analysis then will be the path to a leaf from the root. The data structure of tree node consist of the following information: the characteristics of the protocol, protocol name, protocol code, the lower-level protocol code, data analysis functions linked list. The data analysis function linked list contains all linked lists that are used to analyze intrusion analysis of this protocol, each node in the linked list contains the configuration data.

For the purpose of improving the efficiency and accuracy of intrusion analysis, the network forensic system we presented in this paper is designed to use both pattern matching method and protocol analysis method. The process of network intrusion analysis is as follow: Firstly, to generate the attack characteristics list and protocol analysis list using rule base and protocol analysis library. And then, to interpretate packets from offline files and decode the packets in layers by the protocol. Secondly, to analyze the decoding result using pattern matching method and protocol analysis method, if the intrusion behavior is judged to be sure, the record then will be generated. The process of packet parsing algorithm is to judge each layer protocol of capturing packet according to the sequence of link layer protocol, network layer protocol and transport layer protocols. If the packet is longer than the protocol header, the layer protocol of packet will be removed, otherwise continue reading. The process of intrusion analysis algorithms is to judge whether the packet's IP header pointer is empty, if empty then re-read packets, otherwise the packets will be handled by the TCP, UDP, and ICMP protocols separately. Next, to judge whether there are matching IP and port with the packets, if it is true, then match the packet with the node of attack signature library and protocol analysis library using BM (the Boyer-Moore) algorithm to complete the packet analysis.

E. Application Data Recovery Analysis

Application data recovery analysis is to analyze the application data from network data files, such as the WWW records, email records, Telnet records and FTP records. These applications are very important in the network forensics, for example, all the commands executed by user on the computer can be found out by Telnet recovery analysis, it helps to know the reasons for network incident. The process of application data recovery analysis which has been shown in “Fig. 2” is similar to the receiving process of TCP/IP protocol application. On the left of “Fig. 2” is the process of TCP/IP protocol receiving network application data, and the right is the process of application recovery analysis. The process of TCP/IP protocol receiving network application data is as follow: firstly, network card driver get the Ethernet frame from the card and submit it to IP protocol. Secondly, the head of the link protocol of Ethernet frame will be removed by IP protocol, then make options processing and IP packet reassembly. Finally, make TCP packet reorganization and assemble these TCP packet into application data, such as Web, e-mail, Telnet, FTP, and so on.

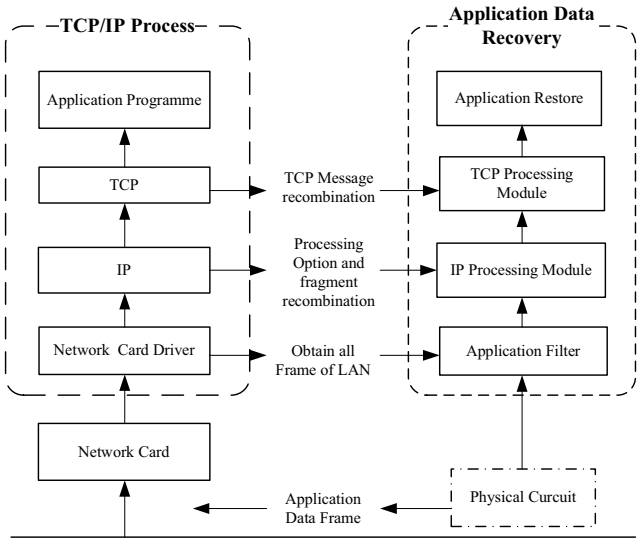

Figure 2. Application Data Recovery Analysis

F. Log Message Analysis

We utilize ASAX method whose characteristics and working mechanism is only processed once for each audit records by rule-based language to analyze the log information analysis, the audit records that have been analyzed will be encapsulated to rules collection[6]. All of these analyzed information can be stored using the C language data structures and can be accessed through external program. The optimized recycling procedure is using activated rule sets to analyze current records and do the same step to the next record. The process of its implementation is as follow: Firstly, user pre-defined the keywords that need to detect, and then establish login failure records rules in a period of time and counting rules, the two rules will be used to traverse log messages, if the mapping records were found, the analysis result of this record then will be stored in its rule chains to make an encapsulated collection of past knowledge, and finally find out the suited records that have attempted to enter the system for the X times t in Y minutes. Secondly, to detect whether some of key documents in the system have been modified. Finally, to detect whether the back door have been installed, and generate log analysis records.

IV. CONCLUSION

In this paper, we have presented a network forensic solution based on Intrusion Detection analysis which can record network intrusion behavior and analyze network data in details. This solution can not only find out intrusion behavior from log information of network data using both static analysis and dynamic analysis methods, but also can transfer system log to the forensics device to prevent hackers to delete the log. This system can record all the network data that across the being forensic computer and store them with time period in accordance with the requirements of the law evidence, so that intrusion behavior will be found out by packet analysis. This processing mode can ensure data integrity and original, so the analysis results of the data possess a high degree of credibility,

this network forensics system provides a technical reference for solving network intrusion problems through legal means.

REFERENCES

[1] Carrier B ,SpaffordE . Getting Physical with the digital forensics investigation.International Journal of Digital Evidence,Winter 2003.

[2] Computer Security Institute, CSI/FBI Computer Crime and Security Survey , Computer Security Institute 2005.

[3] Kornblum J. Preservation of Fragile Digital Evidence by First Responders.In :Digital Forensics Research W orkshop,A ug. 2002.

[4] Brain Carrier,TCTUtils, http://www.digital-evidence.org/.

[5] Andrew Nash,etc., Trans. Zhang Yuqing, Implementation of Public Key Infrastructure (PKI) and Management of electronic security, Beijing, Tsinghua University Press.2002, 38-85

[6] nside Security IT Consulting, Inside Security Rescue Toolkit, http://www.inside-security.de/INSERT_en.html.

.