Network forensic Log analysis

Swati Sinha
IT System and Network security
GTU PG School, Gujarat Technological University
Ahmedabad, India.
swati21sinha@gmail.com

Aditya Kumar Sinha
Principal Technical Officer
CDAC - ACTS
Pune, India
saditya@cdac.in

Abstract - Network forensics log analysis is the capturing, recording, and analysis of network events in order to discover the source of security attacks. An investigator needs to back up these recorded data to free up recording media and to preserve the data for future analysis. An investigator needs to perform network forensics process to determine which type of an attack over a network and to trace out the culprit. In the cyber-crime world huge log data, transactional data occurs which tends to plenty of data for storage and analyze them. It is difficult for forensic investigators to keep on playing with time and to find out the clues and analyze those collected data. In network forensic analysis, it involves network traces and detection of attacks. The trace involves an Intrusion Detection System and firewall logs, logs generated by network services and applications, packet captures. Network forensics is a branch of digital forensics that focuses on the monitoring and analysis of network traffic. Unlike other areas of digital forensics that focus on stored or static data, network forensics deals with volatile and dynamic data. It generally has two uses. The first, relating to security, involves detecting anomalous traffic and identifying intrusions. The second use, relating to law enforcement according to the chain of custody rule, involves capturing and Analyzing network traffic and can include tasks such as reassembling transferred files."Stop, look and listen" systems, in which each packet is analysed in a rudimentary way in memory and only certain information saved for current analysis. On this analysis, we propose to archive data using various tools and provide a "unified structure" based on a standard forensic process. This different unified structured IDS data are use to store and preserve in a place, which would be use to present as an evidence in court by the forensic analysis.

Keywords- *Network forensics, Log Files, Forensic Process,Chain Of Custody.*

*****

I. INTRODUCTION

In the world the crime has increased as investigation works to resolve the cases which included in forensic. Investigators must be able to find and analyze evidence, locate suspects and identify victims. A Figure-by-Figure detail of all forensically includes the legal requirements for collecting Evidence as applicable. Network forensics is scientifically proven techniques to collect, detect, identify, examine, correlate, analyze, and document digital evidence from multiple systems for the purpose of uncovering the fact of attacks and other problem incident as well as perform the action to recover from the attack. Here we will do analysis on network logs. As Network forensics computes the digital evidence which revels the links of digital devices and in between the how and when the crime was taken. The tools, technology and processes required to integrate network evidence sources into the investigations, with a focus on efficiency and effectiveness. An investigation in network and digital devices, working with the IP security could leads to fast catching the victims/attackers. Network security and forensics include the action of monitoring and recording data in transit in order to discover potential attacks. Intrusion Detection Systems (IDS) tools are deployed within networks to perform these actions. The captured data is then examined and analysed possible extraction of the digital evidence. However, analysing such data to produce the evidence can be exceedingly difficult and time consuming. This is because data is always dumped to a log file or databases without a forensic standard structure. Providing auditing for training purposes can also provide difficulties. For instance, when performing a security analysis of the data, system administrators do not have sufficient time to manually record their actions which could be used for these learning and training purposes. While there are several forensic tools available (mostly proprietary's), most of these must be done manually consuming time and resources. In this research, we propose to archive IDS data using various tools and provide a "unified structure" based on standard forensic processes and aim to address this issue by combining several existing tools. These tools will consist of multiple entities (hosts, IDSs, databases, firewalls and attackers) [1].

II. RESEARCH METHODOLOGY

The evolution of network security, as well as its associated forensic processes and related toolsets, is largely driven by recent advances in Internet technologies. As more aspects of our daily lives migrate to online systems and databases where they are subject to criminal activity the need for sophisticated analysis tools is increasing accordingly. Some commonly stated reasons for using network forensics includes specified in [1]:

- Analyzing computer systems belonging to defendants or litigants
- Gathering evidence for use in a court of law

- Recovering data in the event of a hardware or software failure
- Analyzing a computer system after a break-in
- Gaining information about how computer systems work for the purposes of debugging them, optimizing their performance, or reverse engineering them
- Collecting and analyzing live data packets to detect and potentially prevent a malicious attack

This real-time analysis process involves collecting, storing, and tracing data and then recovering the system, all while continuously scanning traffic and logs. As "Fig. 1", shows the recovery process starts with security and then moves into forensic analysis, while carrying out forensic analysis to determine the source of an attack.

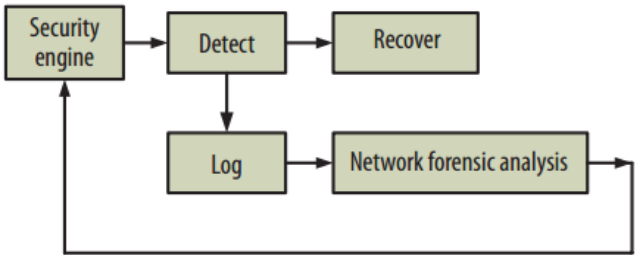

Figure 1: Real-time detection, recovery, and forensic analysis process [1].

A. Security Engine:

The system on which the action would be done on computer system-hardware, OS-software.

B. Detect:

The detection would be as on a crucial system which includes some of the following questions[1]:

1) Who generated the intrusion?
2) What equipment and services were involved in gaining entry?
3) Where did the intrusion come from?
4) What parts of the infrastructure were affected?

C. Recover:

There are many misconceptions about how to retrieve the lost data or deleted data, whether a document was by mistake deleted or an entire drive was formatted, it is the other possibility to recover the client's suspicious data.

From recovery process, a single document to a lifetime of photos, from recovery of one personal account details to an entire hard-disk. Recovery can be performed on a variety of types of media. they are as follows:

1) Hard drives (USB)or hard Disks
2) Smart phones
3) Floppy disks / ZIP disks
4) Secure Digital (SD) cards/Compact Flash (CF) cards
5) Sony memory sticks

D. Log:

Logs containing information relevant to security management are generated by many sources, including:

1) Firewalls
2) Intrusion detection and prevention systems
3) Anti-malware systems, especially centrally managed solutions with aggregated reporting
4) Operating systems
5) Switches
6) Routers
7) Workstations
8) Applications

E. Network Forensic Analysis:

Event log files record information about which users has been accessing specific files, unsuccessfully on to a system, track usage of specific applications, tracks usage of specific applications, track alterations to the audit policy, and track changes to user permissions. Logs are the flow of traffic over the network.

III. PROPOSED WORK

In this project work we propose to archive IDS data using various tools and provide a "unified structure" based on standard forensic processes. This unified structured IDS data will further be presented for optimization and for the forensic analysis.

The propose solution 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. By "Fig.2" whenever an attacker tries to intrude the target host, IDS running on target host detects the intrusion; sends an alert message to security centre as well as log server.

During the analysis phase an investigator recovers evidence material using a number of different methodologies and tools. As shown in "Fig 3". Unique perspective file log which is captured and kept in the database, getting more value out of the network and security infrastructures. As evidence data is the log files that is generated which would be extracted by the "chain of custody" module, which gives the extracted data. Extracted data which is really actionable automatically includes measures security, compliance and incident. The evidence recovered is analysed to reconstruct events or actions and to reach conclusions. The investigator needs to follow proper investigative procedures so that the evidences

 ISSN: 2321-8169
2654 - 2658

recovered during investigation can be produced in a court of law. If the information is extracted accordingly i.e. yes then the result is ready for the use and final reporting is presented.

Figures for proposed module solution:

1) File Logs
2) Evidence Data
3) Any Module
4) Extracted Information
5) Information Extraction/Identification
6) Result
7) Testing
8) Final Reporting

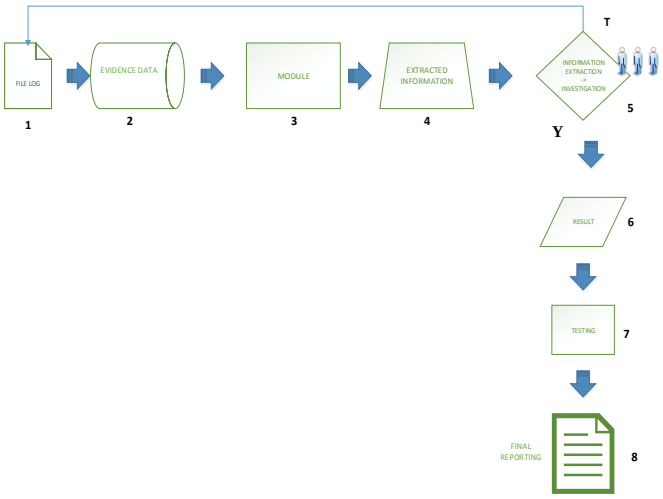

Figure 2 : Archive IDS data Figures

Countermeasure:

- Installation of Anti-virus
- Installation of Firewall and blocking of unwanted ports.

A. Firewall:

Firewalls are software programs or hardware system that filter the traffic that flows into you network or on PC through a internet connection. Firewalls are used to prevent from unauthorized Internet users from accessing private networks connected to the Internet. All data entering or leaving the intranet passes through the firewall, which examines each and every packet and blocks those which not meet the security criteria.

B. Intrusion-detection system (IDS):

An IDS logs everything that's deemed even mildly suspicious. One purpose of IDS is to log an event for further work in order to keep that event from happening again. Here's a list of items that an IDS may log:

1) Port scans
2) Traffic coming in on strange ports or protocols
3) Recognized threats, such as worms or viruses attempting to enter the network
4) Anonymous attempts at using FTP or other services on the network
5) Originating IP addresses of attacks¬
6) Bandwidth usage

IV. Network Forensic Log Analysis Module:

- Understanding Chain of Custody/Data Integrity:

Chain of Custody is the process in which evidence is accounted for and implemented to ensure the integrity of evidence. You need to know how evidence is collected, where it is stored, how it is stored, who has an access, and what procedures have been completed. The appropriate Chain of Custody is followed and documented at all times, which secures the permissibility of your resulting evidence and that your evidence will remain robust under court examination and scrutiny. They provide Forensic Examination Services to Government and Law Enforcement Agencies, Law Firms, Insurance Companies, and Private Investigation Professionals needing to recover digital information and maintaining evidence integrity [11].

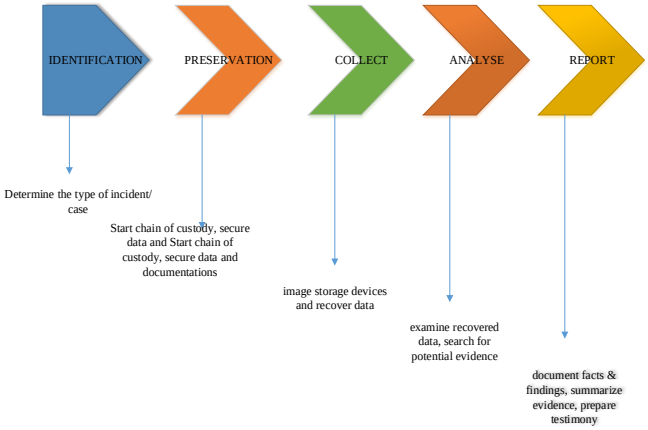

Figure 3 : Chain of Custody (COC) Rule [16]

V. Implementation Using Multiple Logs as Evidence

- Logs from several devices collectively support each other.
- Firewall logs, IDS logs, file systems, deleted files output can contain evidence of an Internet user connecting to a specific server.

Current work is done using some of the following TOOLS/PLATFORM:

TABLE I. TOOLS/PLATFORM

Tools/Platform	Features and Advantages	Attributes
Network Miner	A network forensic analysis tool that can be used as a passive network sniffer/packet capturing tool	Filter & collect
Wireshark	Widely used network traffic analysis tool, forms basis of network forensic studies.	Filter & collect
Ubuntu, Kali	It is a Debian-derived Linux distribution designed for digital forensics and penetration testing	Filter & collect, Reassembly of data stream, Correlation of data, Log Analysis
Xampp control panel	It is an easy to install Apache distribution containing MySQL, PHP, and Perl	It to allow website designers and programmers to test their work on their own computers without any access to the Internet
Putty	It is a free and open-source terminal emulator, serial console and network file transfer application	
Winscp (Windows Secure Copy)	It is a free and open-source SFTP, SCP and FTPclient for Microsoft Windows.	It is secure file transfer between a local and a remote computer. For secure transfers, it uses Secure Shell (SSH) and supports the SCP protocol.

F. Analysis Work:

On the basis of analysis done by comparing the tool on the website and the data collected through different tools will be presented to the court as same as it origin according to the forensic process with COC.

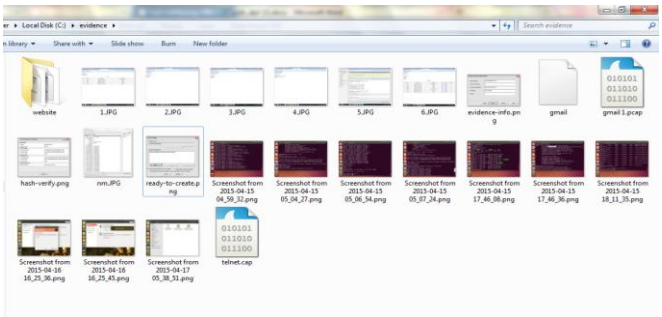

Figure 4 : Evidence Collected

There must be an accurate and complete log of digital evidence, the legal process and the law enforcement agencies that will require much more complete information. Signature of the object, the identity of all parties who interact with the evidence, the location where the evidence is handled, the time of access to the evidence and all the descriptions that contain any access to evidence is some information that is needed in the process of recording digital evidence .

- A description of the from Figure 3 is as follows:

1) Investigator forecloses evidence.
2) For certain tools, it has been performed the acquisition process to get the image file.
3) The acquisition process can be done online (triage forensics) or offline. The acquisitions could use all the tools and instruments depending on the nature and characteristics of evidence found.
4) After the acquisition process is completed, the evidence is collected in a folder and then given the label and recording.
5) Then evidence is then submitted to the register.
6) The results of the acquisition process are in the form of image files to a format that suits the equipments and tools used when acquiring evidence.
7) Image file as evidence is not stored in a personal computer of the investigator but is stored in a secured storage system.
8) If the investigator requires evidence for the benefit of his/her investigation, he or she must go through certain procedures to be able to get access to the evidence that has been stored in the evidence room.
9) If another investigator is interested to do an analysis of the physical and digital evidence, he/she must go through a specific mentioned mechanism.

To deal with such attacks, several security solutions as well as mechanisms are available. But these solutions are required to be updated sometimes upgraded to prevent newly introduced threats. Some of the security solutions are listed below.

TABLE II. AVAILABLE SECURITY SOLUTIONS

Sr. No.	Security Solutions	Description
1.	Digital Certificates	Ensures the authenticity of sender. Protects against Authorization threats and Masquerading.
2.	Firewalls, Deep Packet Filtering	Controls the network communication according to defined rules. Protects against IP spoofing, DoS attacks.

VI. CONCLUSION

On this analysis, we propose to archive data using various tools and provided a "unified structure" based on a standard forensic process and a module used i.e. chain of custody which has increased the efficiency and the time. This different unified structured data are use to store and preserve in a place and would be use to present as an evidence in court by the forensic analysis.

REFERENCES

[1] Ray Hunt & Sherali Zeadally "Network forensics: analysis is of techniques, tools, and trends" University of South Australia, University of the District of Columbia, 2012.

[2] Ray Hunt, Malcolm Shore "Network Forensics and Log Files Analysis" A Novel Approach to Building a Digital Evidence Bag and Its Own Processing Tool , University of Canterbury Department of Computer Science and Software Engineering , September 30, 2011.

[3] ILKYEUN RAA "Forensic Logging System Based On A Secure Os " Dept. of Computer Science and Engineering, University of Colorado Denver 1200 Larimer St. Campus Box 109. Denver, CO 80204, U.S.A. Ilkyeun.ra@ucdenver.edu , http://carbon.cudenver.edu/~ikra , TAE-KYOU PARK Dept. of Computer and Information Science, Hanseo University Seosan, 356-706, South Korea , tkpark@hanseo.ac.kr .

[4] Mr. Sudhakar Parate, Ms. S. M. Nirkhi "Review of Network Forensics Techniques for the Analysis of Web Based Attack" M.Tech Scholar ,Asst. Professor ,Department of Computer Science and Engineering, G.H.Raisoni College of Engineering Nagpur, India.

[5] Simson Garfinkel, "Network Forensics: Tapping the Internet"

[6] Arati Baliga, Nitin Gupta, Lev Kaufman, Prashant Mekaraj, Andrew,Tjang, WenyuanXu "Network Monitoring and Forensics".

[7] Bhavesh Patel, Jazi Eko Istiyanto, Ahmad Ashari, Subanar, done the "Comparative Analysis of Network Forensic Systems" were the Student of Government Engineering College, Gandhinagar, Gujarat, India; Sanjay.M.Shah Professor of Government Engineering College, Gandhinagar, Gujarat, India.; Sameer Singh Chauhan Asst. Professor Sardar Vallabhbhai Institute of Technology, Vasad, Gujarat, India AND, Department of Computer Science and Electronics, Department of Mathematics, Faculty of Mathematics and Natural Sciences, Gadjah Mada University, Yogyakarta, Indonesia {jazi,ashari}@ugm.ac.id, subanar@yahoo.com

[8] Imam Riadi "Log Analysis Techniques using Clustering in Network Forensics" Department of Information System, Faculty of Mathematics and Natural Science, Ahmad Dahlan University, Yogyakarta, Indonesia imam_riadi@uad.ac.id.

[9] Komal Barhate, Jaidhar "CDAutomated Digital Forensic Technique with Intrusion Detection Systems" Department of Computer Engineering, Defense Institute of Advanced Technology, Pune - 411025, India. mcse2011_komal@diat.ac.injaidharcd@diat.ac.in .

[10] Vasami "A Unified Model to Cherish Privacy in Database System- libre" 2014

[11] Yudi Prayudi, Ahmad Ashari, Tri K Priyambodo "Digital Evidence Cabinets: A Proposed Framework for Handling Digital Chain of Custody ", International Journal of Computer Applications (0975 – 8887) Volume 107 – No 9, December 2014

[12] Mark Scanlon and Tahar Kechadi, "Digital Evidence Bag Selection for P2P Network Investigation", School of Computer Science and Informatics,University College Dublin,Belfield, Dublin 4, Ireland.

[13] "Network Forensics: Tapping the Internet" http://www.oreillynet.com/pub/a/network/2002/04/26/nettap.html.

[14] "Secure state Analysis" http://forensicanalysis.com .

[15] Sherri Davidoff Jonathan Ham "Network Forensics (Tracking Hackers through Cyberspace".

[16] http://www.natldf.com/services.php