International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) ISSN: 2395-5325
Volume 3, Special Issue 3 (September '2017)
Proceeding of - International Conference on Recent Trends in Computational Life Science and Information Technology,
Conference held at Tiruppur Kumaran College for Women,Tirupur,Tamilnadu, India.

INTRUSION DETECTION SYSTEM IN DIGITAL FORENSICS

Dr. N. Sasirekha,
Associate Professor,
PG Department of Computer Science,
Vidyasagar College of Arts and Science,
Udumalpet,Tamilnadu,India.

A.Shanthi Sona,
Assistant Professor,
Department of Computer Science,
Tiruppur Kumaran College for women,
Tirupur.Tamilnadu,India.

Abstract: Internet has changed and improved the way of working in organizations and businesses, at the same time this large network also opened doors for attackers as new attacks are emerging day by day. To protect the organizations and systems from these attacks, network security comes into action. The need for computer intrusion forensics arises from the alarming increase in the number of computer crimes that are committed annually. After a computer system has been breached and an intrusion has been detected, there is a need for a computer forensics investigation to follow. The goal of this paper is to explain the advantages and disadvantages of computer intrusion forensics. The paper will look at how intrusion detection systems can be used as a starting point to a computer forensics investigation. Also, the ways to preserve and recover data during a computer forensics investigation will be explored. A discussion of how some of various software tools that are used in a computer forensics investigation will be included. Last, the paper will explore ways that an intrusion detection system can be used in correspondence with computer forensics.

Keywords: Intrusion detection system, digital forensics, digital evidence, forensic analysis.

I.INTRODUCTION

Intrusion forensics is a specific area of Computer forensics, applied to computer intrusion activities. Computer forensics, which relates to the investigation of situations where there is computer-based (digital) or electronic evidence of a crime or suspicious behavior, but the crime or behavior may be of any type, quite possibly not otherwise involving computers. Intrusion detection uses standard computer logs and computer audit trails, gathered by host computers, and/or information gathered at communication routers and switches, in order to detect and identify intrusions into a computer system. Successful detection of intrusion is based either upon recognition of a known exploitation of a known vulnerability or upon recognition of unusual or anomalous behavior patterns or a combination of the two. Computer forensics on the other hand is concerned with the analysis of any information stored by, transmitted by or derived from a computer system in order to reason post hoc about the validity of hypotheses that attempt to explain the circumstances of an activity under investigation. Computer forensics therefore, covers a much broader scope of activities than does intrusion detection, the scope of the latter being limited to reasoning about activities or detecting activities relating to computer system abuse. Computer forensics involves the preservation, identification, extraction, documentation and interpretation of C computer data. Computer forensics is usually used when a crime has been committed or an inappropriate activity has taken place. Some common examples of when computer forensics is used are:

- Identity theft, such as stolen credit cards numbers and social security numbers.
- To reveal if trade secrets were stolen from an organization.
- Investigate a hackers attack on a computer system.
- Finding evidence of child pornography.
- For divorce proceedings, evidence of a cheating spouse.

I. DIGITAL FORENSICS

Computer forensics is used to bring to justice, those responsible for conducting attacks on computer systems throughout the world. Because of this the law must be followed precisely when conducting a forensics investigation. It is not enough to simple know an attacker is responsible for the crime, the forensics investigation must be carried out in a precise manner that will produce evidence amicable in a court room. For computer intrusion forensics many methodologies have been designed to be used when conducting an investigation. A computer forensics investigator also needs certain skills to conduct the investigation. Along with this, the computer forensics investigator must be equipped with an array of software tools. Computer forensics involves many common investigative techniques used by law enforcement. The only difference is they are used on digital media. The main goal of a computer forensics investigation usually involves a conviction in either criminal or civil court. Great care must be taken in the preservation and recovery of data. An organization should build their security policy around the event that it is inevitable that computer forensics will be needed in the future. If an enterprise has a plan in place for when an intrusion takes places, it will greatly aid the organization into the forensics process. All employees of an organization should be trained on what to do in the event of an intrusion. Failing to provide employees with training and written procedures can jeopardize a computer forensics investigation. For instance, an employee may think he is aiding in helping to contain an incident and in actuality may be damaging evidence. Along with the typical computer user of the organization, system administrator should also be trained. While the system administrator knows a great deal about their system, they may not have the proper training of what to do in the event the computer forensics. For these

reason the security policy of an organization should contain what to do in the event that computer forensics is needed. The need for computer intrusion forensics arises from the event that an intrusion into a computer system has occurred.

According to the CERT web site a computer intrusion is, "Any intentional event where an intruder gains access that compromises the confidentiality, integrity, or the availability of computers, networks, or the data residing on them."

Intruders can be classified into three types :

- **Masquerader:** An individual who is not an authorized to use the computer and who penetrates a system's accesscontrols to exploit a legitimate user account.
- **Misfeasor:** A legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges.
- **Clandestine user:** An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection.

The amount of damage done by an intruder to a system can vary greatly. Some intruders are malicious in nature and others are just curious and want to explore what is on a local network. Computer users must protect themselves from intrusion. While there are no 100% effective methods of eliminating intruders completely, some methods must be used to reduce intrusions. In the event that an intrusion has taken place the last line of defense is an intrusion detection system. An intrusion detection system can alert the system administrator in the event that the system has been breeched. Once the intrusion detection system has detected an event, an intrusion forensics investigation should be conducted to note the extent of the intrusion and any damages that may have occurred and to locate the source of the attack. Computer intrusion forensics will be an emerging field of study in the twenty-first century. The need for computer forensics will continue to increase as computers become even more prevalent in society. As further research takes place in this field, computer forensics will continue to move from being an art, towards a scientific field.

Intrusion Detection System (IDS) and Digital Forensics (DF) are used in computer and network security to protect and secure the system, network, or organizations. First one is used to detect the intrusion or attack in order to prevent the damage in the given system or network, whereas later one is used to analyze the attacked or compromised system in order to find the amount of damages occurred, cause of the attack and strategies used in the attack. Both intrusion detection system and digital forensics have an application in one another. Digital forensics is a process of collecting, analyzing, and presenting digital evidences about attack and intrusion detection system can be used to produce evidences that can be used as evidence. Intrusion detection system is one of the most important and popular sources of digital evidence as it enables the administrator to collect the evidence about the attack by providing the information about the attack. The evidences collected with the help of intrusion detection system are the real time and practical one, as they are collected at the same time when an attack is detected. Such evidences contain the most of the important information about the attack such as network connection, running processes, open files, system calls, the amount of data flowing, memory use, etc. The evidences produced by intrusion detection systems directly are the documentary evidences and can be used in legal proceedings with a testimony of the person responsible to generate such evidence. On the other hand digital forensic techniques can be used in intrusion detection process. This process is known as network forensics, which deals with volatile and dynamic information. Network forensics generally have two uses. The first related to security, in which network is monitored for anomalous traffic and intrusions are identified. The second use of network forensics is related to law enforcement. Network data is more unpredictable and volatile as compared to computer forensics, where data containing evidence is generally preserved on disk.

A network forensics system is easy to implement, in practice many obstacles in building a network forensics system. There are at least two kinds of obstacles in building a system that is network forensics technical and socio-economic.

1. **Data Collection**
   It is an addition to network forensics system has a function to monitor network activity should also be able to collect all the data passing through the network. Data collected and saved may be used to conduct an investigation if there is an attack or threat, and the results of those investigations can also be used as digital evidence if it would be conducted legal measures as a result of the implications of an attack or a threat to the network. Additionally, it will also have problems with the increasing data traffic on the network, consequently needed a data storage system that can accommodate the data if it happens.
2. **Data Retention**
   Data collected possibility should be maintained or stored for a considerable period of time. It is an effect on the amount of data that can be accommodated by the system network forensics. Therefore we need a data management can reduce the amount of data stored without loss of valuable forensic information.
3. **Data Retrieval**
   During the treatment, the investigation or analysis system should be able to determine the location of the data required in the wide area network. As mentioned earlier, the data stored in the system forensics can be very large in number. Therefore we need a protocol to determine the location of the necessary data quickly.
4. **Privacy**
   Surveillance network with user privacy will always be the opposite. It is due to the system overall forensic examination is required of a system that can make the user uncomfortable. The solution is to investigate all the traffic data, but only store information that is necessary for forensic only. This is possible because of the processing speed of today's computers faster than the speed of storing data. By doing so, the storage of information that is very personal and less valuable to forensic system can be reduced.
5. **Economy**
   The development of a judicial system also depends on the profit from the service provider. It will greatly affect the price of a legal system. Forensic system is also very useful in reducing the level of threats and attacks against the organization or company network, so as to reduce the

losses suffered as a result of the threat. Increasingly the world is becoming dependent on the information derived from digital sources, computer systems, and networks involved in storing, processing, and transmitting data. This growing dependence drives development to advance required technology. Figure (i) shows the area where digital forensic comes into action.

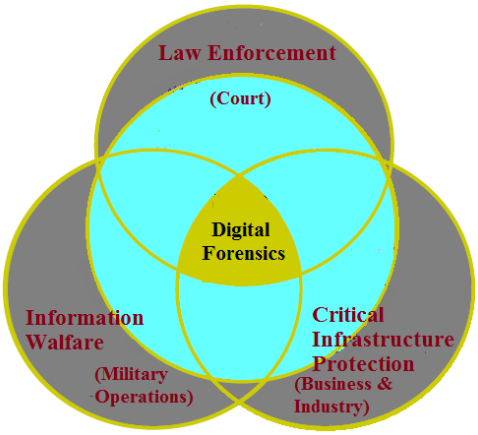

Figure 1: Area of application of digital forensics.

Fundamental principle in Digital forensic investigation

Core IT Security has fundamental principles as confidentiality, Integrity and Availability. The core principles in digital forensic investigations are as follows:

1. Reconnaissance:

This is an observation of actions to be taken to secure and collect digital evidence in such a manner that they should not affect integrity of evidence. For this, forensics investigator uses different tools, methods, and practices specially developed for that and store on different storage media to make readable evidence .

2. Reliability:

Data extraction is not simply to save files to a disk or copying the data. Evidence-chain should be preserved during extraction, analysis, storage and transportation of data to make the forensic process reliable. Trained persons should be appointed to conduct an examination of digital evidence.

Relevancy: Relevancy of the evidence with the case may affect the usefulness and weight of the evidence, even though for admissible evidence . For better and controlled investigation, advice from legal practitioner should be taken on what should be collected, time and cost spent during the process .

II. DIGITAL FORENSIC MODEL

Several models for digital forensic investigation have been proposed. One most popularly used model of them is given in Figure (ii).

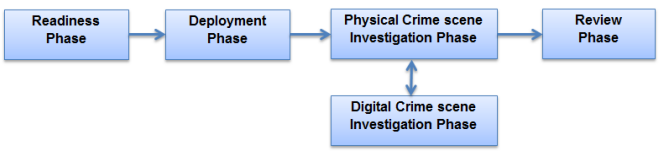

Figure 2 :Digital Forensic Investigation Model.

1. Readiness phases

The concept of forensic readiness for a system describes the capability of the system to efficiently collect credible digital evidence that can then be used in legal proceedings .

Readiness phase is responsible to verify the ability of infrastructure and operations to support an investigation completely.

It combines two phases:

Operations Readiness phase, that ensures human capacity, whether it is capable or not to deal with incoming incidents.

Infrastructure readiness phase, that ensures the infrastructure is sufficient or not to deal with incoming incidents.

2. **Deployment phases**

It provides a mechanism and set up for detection and confirmation of an event. It also combines two phases: Detection and Notification phase, that detects the incident and Notify investigator about it.

Confirmation and Authorization phase, that verify the occured incident and take authorized legal approval.

3. Physical Crime Scene Investigation phases

This phase is responsible for collection and analysis of physical evidence and reconstruction of the actions that took place during the occurrence of events. It contains six phases such as preservation phase, survey phase (taking photographs, sketches, and videos), documentation phase, search collection phase, reconstruction phase, and presentation phase.

4. Digital Crime Scene Investigation phases

This phase is responsible for the collection and analysis of the digital evidence found either from the previous phase or from any other source of evidence collection. This phase is similar to physical crime scene investigation phases, but this phase mainly focuses on the digital evidence.

5. Review phase

This phase reviews the whole investigation process and identifies areas where improvement is needed.

III.NETWORK FORENSICS TOOLS

Network forensics tool is the application used for the forensic experts who used to do things related to forensic such as monitoring and audit on the network. Toolkit for forensic testing allows investigators to gather and analyze data such as E-Detective, NetFlow v5 / 9, netcat, NetDetector, tcpdump, Wireshark / Ethereal, Argus, NFR, TCPWrapper, sniffer, nstat, and tripwire.

Some examples of network forensic tools

1. Packet sniffers

Packet sniffers are used to analysis network traffic. Sniffers can be used when analyzing a live attack on a computer system. A sniffer captures the packet on a network and can subsequently be used to analyze a live attack. By analyzing the individual packets, it may be possible to locate the address where an attack is coming from. One problem with this approach is it is possible to spoof an IP address. Some popular packet sniffers are tcpdump, dsniff, and ethereal. A sample output from program ethereal is shown in Figure (iii) .

International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) ISSN: 2395-5325
Volume 3, Special Issue 3 (September '2017)
Proceeding of - International Conference on Recent Trends in Computational Life Science and Information Technology,
Conference held at Tiruppur Kumaran College for Women,Tirupur,Tamilnadu, India.

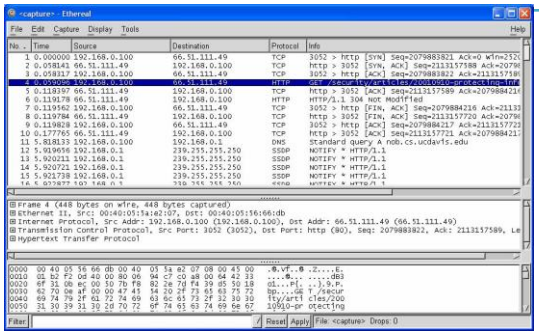

Figure3: Ethereal sample output

2. Wireshark

An analyzer and monitoring network that is popular. The features in Wireshark, such as:

- Can checks for hundreds of protocols in depth
- Able to capture direct and analyzed offline
- Multi platform can run on Windows, Linux, Mac OS X, Solaris, FreeBSD, NetBSD, and others.
- Data networks have been captured can be displayed via the GUI or via the TTY-mode.
- Can filter the view with many filter options.
- Can read and store different formats.

3. Netcat

It is a utility tool that is used for a wide range of issues related to TCP or UDP protocol that can open TCP connections, sending UDP packets, listen on the TCP and UDP port -Port, scanning ports, and by IPV4 and IPV6. This Netcat typically used by hackers to connect back to the target system so that hackers gain root access through the port that has been set by the hacker.

4. E-Detective

It is an interception system that makes the process of the Internet in real-time, monitoring and forensics systems that capture, code reading, and restore some types of Internet traffic. These systems are typically used in corporate Internet and monitor behavior, audit, storage of records, forensic analysis, and investigations. E-Detective can read the code, reassembly, and recover various types of Internet Applications and services this example, Email, Webmail, Instant Messaging, File Transfer, Online Games, Telnet, HTTP, VOIP, and others.

III.SOFTWARE TOOLS

Preserving and recovering data in an investigation is done with a large assortment of software tool. A computer forensics investigator is severely limited in their capabilities without the proper tools. There are many different categories of software tools available for use in a computer forensics investigation. For instance there are tools to analyze a drive, and tools to analyze a network. There are also three main variations of software that is generally used: commercial, open source, and operating system utilities. No single tool can be used in all situations, so a computer forensics investigator will use many different software programs. The investigator must select the correct tool depending on the objective to be accomplished.

IV.HARDDRIVE TOOLS

First investigation is to determine information about the hard drive on the suspect system. The investigator should have software tools to find general information about a hard drive. The tools should give information about the number of partitions and file systems used on the drive. Partition Magic is a good commercial program that can be used. One nice feature of Partition Magic is that a drive can be examined in read-only mode . Operating system programs such as fdisk for Windows or fsck for UNIX can also be used for this purpose. A tool such as Partition Magic is usually able to determine a greater number of different types of file systems than the tools provided by the operating system.

It is common to use the MD5 hash algorithm to take the message digest of files to be compared. The message digests are then used to validate the integrity of files. The values are also used in court to prove that the files were not modified during the investigation. A frequent use of message digest values can be taken of all the library files of the operating system when it is installed. At a later time, the current hash values can be compared with the previous values to see if any changes occurred. If there are discrepancies between the values, the system files have been changed. This method is used to help locate malicious code. The one problem with using message digests is they can't validate the integrity of files that are changed frequently such as logs. Hash values are best suited for files that stay static such as system library function. Tripwire is a popular commercial program that takes the hash values. The program then automates the process of comparing the message digests of files.

Hex Editors can be used to examine clusters on the hard drive. A hex editor can look at individual sectors of a hard drive and/or examine individual files as a whole. Files that are deleted can be recovered by a hex editor. A hex editor will give the hex values that are contained on a hard drive. As explained before it is possible to examine the swap, slack and deleted space on a drive and reconstruct the files. It is also possible to view the ASCII text converted form hex directly in many hex editors. Figure (iv) shows a sample output of a Hex Workshop, a hex editing program.

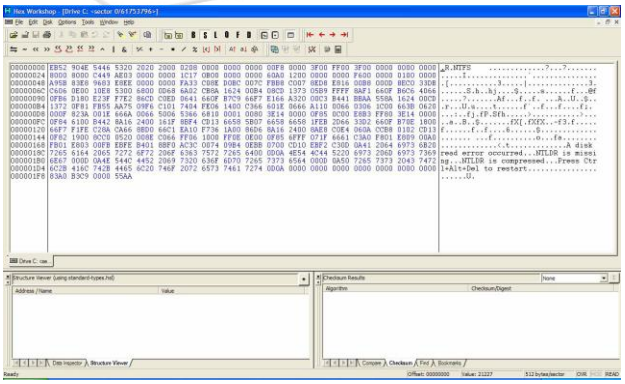

Figure 4 : Hex editing program

There are several difficulties in addressing Intrusion Detection Systems with Computer Forensics. First, the theoretical requirements of an IDS in terms of performing its primary mission may be at odds with the requirements of collecting an preserving forensic evidence. The primary mission of an IDS is to detect and respond to security incidents. The definition of a security incident should be, at least in part, determined by the organization's security policy. Therefore, the detailed

definition of the IDS' primary mission is partially determined by the security policy, not by some overarching standard or generic procedure. The result is that there can be a wide disparity among requirements for an IDS from organization to organization. That contrasts significantly with the relative static set of requirements for developing and managing evidence for use in a legal proceeding.

A second difficulty is that an IDS, by design, does not manage its information in the sense that a forensics systems does. There is a requirement within a forensic system for, among other things, the maintenance of a chain of custody whereby all evidence can be accounted for and its integrity attested to from the time of its collection to the time of its use in a legal proceeding.

The third difficulty deals with the architecture of the IDS. The ability of a program to perform widely disparate tasks implies an architecture that may or may not be present currently in an IDS. Thus, there develops the need for a standard architecture for intrusion detection systems that also are capable of forensic data management.

A major problem with the current approaches to anomaly detection is that it is difficult to define normal user behavior. Misuse detection approaches (Rule-Based), on the other hand, detect only known attack patterns with high accuracy. In a dynamic environment it will be almost impossible to created user profiles that determine the normal behavior. Therefore, it would be better to look at intrusion detection systems that observe the behavior of process rather than users. Intrusion detection tools of the future must be able to more effectively deal with detection evasion techniques and encrypted network traffic. An automated Intrusion Detection System for detecting anomalous behavior will help tremendously to alleviate some of the burdens that are placed on Security Administrators.

V.CONCLUSION

Crimes involving network weaknesses often happen anywhere. Computer system security using firewalls and IDS is now no longer sufficient, so that the necessary forensic capability in network security system implementation. Firewalls can be deceived by a virus or hacker attack on the system. Network forensics will conduct further searches of the system that has been disturbed. There will be a trade-off between the forensic system with privacy therefore we need a policy of legal system that will be used by a company or organization. Network forensic, can be combined together with ids for further works to make system leaks easily addressed.

VI.REFERENCES

[1] B. Ruchandani, M. Kumar, A. Kumar, K. Kumari dan A. Sinha, "Experimentation In Network Forensics Analysis," dalam Proceedings of the Term Paper Series under CDACCNIE, Bangalore, India, 2006.

[2] A. Lubis dan A. P. U. Siahaan, "WLAN Penetration Examination of The University of Pembangunan Panca Budi," International Journal of Engineering Trends and Technology, vol. 37, no. 3, pp. 165 - 168, 2016.

[3] N. Meghanathan, S. R. Allam dan L. A. Moore, "Tools and Techniques for Network," International Journal of Network Security & Its Applications, vol. 1, no. 1, pp. 14-25, 2009.

[4] Behrouz A Forouzan. *Cryptography & Network Security*. McGraw-Hill, Inc., 2007.

[5] Xin Yue, Wei Chen, and Yantao Wang. The research of firewall technology in computer network security. In *Computational Intelligence and Industrial Applications, 2009. PACIIA 2009. Asia-Pacific Conference on*, volume 2, pages 421–424. IEEE, 2009.

[6] Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinou. Sensor network security: a survey. *Communications Surveys & Tutorials, IEEE*, 11(2):52–73, 2009.

[7] S Zargar, James Joshi, and David Tipper. A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks. 2013.

[8] KeWei, Muthusrinivasan Muthuprasanna, and Suraj Kothari. Preventing sql injection attacks in stored procedures. In *Software Engineering Conference, 2006. Australian*, pages 8–pp. IEEE, 2006.

[9] Tarek S Sobh. Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art. *Computer Standards & Interfaces*, 28(6):670–694, 2006.

[10] Abdallah Ghourabi, Tarek Abbes, and Adel Bouhoula. Honeypot router for routing protocols protection. In *Risks and Security of Internet and Systems (CRiSIS), 2009 Fourth International Conference on*, pages 127–130. IEEE, 2009.