Role of Intrusion Detection System in Computer Forensics and Challenges Involved

Shikha R. Agrawal
Department of Computer Engineering
AISSMS'S Institute of Information Technology, Pune, Maharashtra, INDIA

Abstract- *With the alarming increase in the cases of computer intrusion the need of computer forensics has arrived. Computer forensics provides a legal procedure of investigation when computer is detected for intrusion.*

Computer forensics outlines legal justice system which is needed to address the issues of security breach throughout the world. The laws and legal procedures must be followed properly in order to collect evidences related to intrusion. It is not sufficient to know the culprit, all the evidences must be collected in forensically sound manner to prove charges against offender in court room. The forensic investigator must use defined forensic processes and must be equipped with forensic tools to collect evidences.

Day by day our dependency over the network is increasing exponentially. So necessary primitives are required to secure systems against any computer intrusion. Intrusion detection system are developed to indentify intrusion and to execute preventive measures.

Keywords- Computer Forensic, Digital Evidence Intrusion Detection System.

I. INTRODUCTION

Computer Forensics is an area of computer science which became increasingly important in daily aspect and widely used in current century for collection of evidences and investigation of cyber attacks. Computers have given criminals opportunity to carry out their misdeeds using anonymity.

The computers forensic will typically investigate the computers either used to commit the crime or which are the targets of the crime. Intrusion forensics is a specific area of Computer forensics, applied to computer intrusion activities.
Computer forensics is the investigation of scenario 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. Whereas Intrusion forensics relates to the investigation of attacks or suspicious behavior directed against 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.

II. PROBLEM DEFINITION

Computer forensics and digital evidences are emerging fields of research and requires standardization and legal procedures to be defined for them. And Intrusion is a common threat related to cyber security. The goal of the paper is to explain the various sides of computer intrusion and how an intrusion detection system can be used as an initial point for forensic investigation and the ways of preserving and recovering digital evidences related to intrusion.

1. COMPUTER INTRUSION

"Computer intrusion is classified as any intentional event where an intruder gains access that compromises the confidentiality, integrity, or the availability of computers, networks, or the data residing on that computer or network."

According to the William Stallings book Cryptography and Network Security, intruder can be classified into three categories [Stallings 2003]:

Masquerader: An individual who is not legitimate user of a computer penetrates a system's access controls to exploit a authorized to user.

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 damage incurred to a computer system by various types of intrusion may vary from case to case. Some

intrusion may be malicious in nature while in other intruder's intention is to explore the system to out of curiosity. There is no system available which can guarantee complete intrusion protection but some methods can be employed to reduce intrusion. So to defend the system from Intrusion Detection System are available. An Intrusion Detection System Provide alerts to System administrator if the system's security is breeched. Once an event of intrusion is detected forensic investigation need to be carried out to identify the extent of intrusion and damages incurred and to locate the suspect of attack.

2. COMPUTER FORENSICS

Computer Forensics involves the preservation, identification, extraction, documentation and interpretation of computer data [Kruse II and Heiser 2002]. Computer forensics is usually used when a crime has been committed or an inappropriate activity has taken place. The main goal of a computer forensics investigation usually involves a conviction in either criminal or civil court. During an investigation, procedures must be followed precisely so evidence is amicable in court.

3. INTRUSION DETECTION SYSTEMS AND A VIEW TO ITS FORENSIC APPLICATIONS

The ultimate goal of Intrusion Detection is to identify, preferably in real-time, unauthorized use, misuse, and abuse of computer systems by both systems insiders and external penetrators. The ability to obtain a fingerprint of system users and their typical behavior is imperative in order to acquire some hold on identifying the perpetrator.

The study of available log files would always be uses as fundamental in evidence collection.

Intrusion detection systems can form a starting point that can be used by a computer forensics investigator.

3.1 DATA PRESERVATION, RECOVERY AND EXAMINATION

From the forensic perspective rich sources of digital evidences are found at the following places:

1. Hard drives
2. Memory
3. System logs
4. Email servers
5. Network traffic
6. Intrusion detection systems

If possible the computer system that holds the evidence should be seized. The investigator may not always be able to confiscate the computer, for instance it may be hard to justify taking a live server down for analysis. When possible, the best solution is to power the computer down and preserve the data on it. One drawback of powering down a computer is that evidence which may reside in memory will be lost when the system is shut down.

3.2 PRESERVING DATA

The next step that should be taken in an investigation, after the evidence has been seized, is data preservation. The data should be put on a write protected medium. Hash functions should be used to authenticate the integrity of the data. There are programs available that can be used to take a hash value of the entire drive. If the data is not properly preserved and the case makes it to court, a conviction will be unlikely if the data is contaminated, even if there is substantial evidence. It is common to copy data to a read-only medium such as a CD-Rom to prevent the data from being altered. Another solution is to make a copy of a hard drive to another hard drive.

3.3 RECOVERING DATA

After the data has been preserved, the next step is recovering and examining the data. There are many techniques that a suspect can use to hide information, depending on the level of skill of those in question. Data can be located in odd places or have misnamed files. Files may be protected by passwords. While passwords may deter many users, the investigator should be able to recover these files. Password cracking programs can be used to gain access to password protected files. The evidence sought after may be encrypted. It is usually infeasible to try to crack encryption unless weak encryption is used. The evidence sought after may have been deleted from the hard drive. It is usually possible to retrieve deleted files. If a file is deleted, it will still reside on the hard drive unless it is over-written with a new file. So it is possible to recover this data by reading the individual sectors of a drive. Various software tools and techniques can be used in the recovery.

3.4 SYSTEM LOGS

While a great deal of information can be gained from the host computer, information also can be obtained from a server. The majority of events that take place in a computer system are recorded in log files on servers. By failing to collect the system logs, valuable information can be overlooked. Logs can contain information such as user name,

password, access time, device used, functions performed, and other information depending on the type of log Firewalls and Intrusion Detection Systems have logs that can be evaluated for suspicious activities. Many network routers also have logs that the investigator can examine to reconstruct evidence. If a computer is not set up to log many activities the amount of evidence found in the system logs will probably be minimal. Also, the more activities logged, the harder it will be for someone to cover their tracks.

3.5 SOFTWARE TOOLS

Preserving and recovering data in an investigation is done with a large assortment of software tool. 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.

3.6 HARD DRIVE TOOL

An image of a hard drive should be taken before the examination of data takes place. The hard drive in question should never be analyzed in an examination; instead an exact copy should be examined.

For this reason, a good drive imaging program is needed. Many backup programs only backup files and don't copy slack space, unallocated areas, and swap files

A drive imaging program should be used that will create a bit copy of an entire drive. 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.

3.7 NETWORK TOOLS

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. Some popular packet sniffers are tcpdump, dsniff, and ethereal. By using IDS, an attack on a system can be reconstructed and examined. An intrusion detection system is one of the first places that should be examined when starting an investigation. By using IDS it may be able to determine how an attacker gains access to the system. A popular open source IDS is snort.

3.8 TOOLS TO SEARCH AND RECOVER FILES

Searching through text files is crucial in an investigation. There is a wide-range of text searching programs that are used to find files containing certain key words.

Recovering files may also involve the need for cracking passwords. Many password cracking programs can be used, depending on the application that must be cracked. There is a password cracking programs for virtually any program that uses a password.

3.8.1 ALL PURPOSE TOOLS

Programs made specifically for forensics investigations are available, such as EnCase and ForensiX. EnCase is the industry standard software used by law enforcement. Encase is probably the most powerful forensic tool available on the market. Encase provides the majority of the tools discussed above.

4 EVALUATION AND RESULTS

There are several difficulties in addressing Intrusion Detection Systems with Computer Forensics. The primary mission of IDS is to detect and respond to security incidents. The result is that there can be a wide disparity among requirements for an IDS from organization to organization.

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 IDS. Thus, there develops the need for a standard architecture for intrusion detection systems that also are capable of forensic data management.

An automated Intrusion Detection System for detecting anomalous behavior will help tremendously to alleviate some of the burdens that are placed on Security Administrators.

III. CONCLUSION

A survey of the field of computer intrusion forensics is given in this paper. Basic overview of intrusion detection systems and how they relate and aid in computer forensics was discussed. Furthermore, some basic steps need to preserve, recover and examine data were discussed. Last, a wide-range of software tools were examined that can aid in the investigation process. Current intrusion detection systems operate at high level of data manipulation and are ineffective for detecting intrusions that can occur at a low network level. All the intrusion detection approaches use input in the form of audit data created by the operating system. The audit data provided in most cases tends to be problematic; special programs such as data mining are needed to subtract meaningful data from the records. Today's intrusion detection systems are not yet intelligent enough - a human still needs to interact too much in setting up and maintaining intrusion detection systems. Also, it might be possible in the near future to combine firewalls, computer intrusion forensics and anti-virus scanner technologies to form a robust Intrusion Detection Systems (IDS) that can detect all types of intrusions in real time. An automated system for detecting anomalous user behavior will help alleviate a, sometimes nrealistic, burden on systems administrators. However, these automated systems are not only useful during a violation but can be an invaluable forensic tool after the fact. 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. Evidence of the increased popularity of computer forensics is a small number of colleges have begun to offer programs in computer forensics, such as University of Central Florida and University of Texas at Dallas. Computer forensics investigators will become an integral part of an organizations security department. The paper explored a wide-range of areas dealing with computer forensics.

REFERENCES

[1] Stallings, William- Cryptography and Network Security: Principles and Practice 3rd Edition. Upper Saddle River, NJ: Prentice Hall, 2003.

[2] Stallings, William- Data and Computer Communications 7th Edition Upper Saddle River, NJ: Prentice Hall, 2004.

[3] Biermann, E., Cloete, E., and Venter L.M- "A comparison of Intrusion Detection systems". Computer & Security, Vol. 20, Issue 8, 1 December 2001, Pages 676-683

[4] Broucek, V. & Turner, P.- "Research in Progress: Risks and Solution to Problems Arising from Illegal or Inappropriate On-line Behaviors: Two Core Debates within Forensics Computing" EICAR Conference Best Paper Proceedings. 2002. pp. 206-219. Copenhagen: EICAR