International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 1 –NOVEMBER 2014.

Computer Intrusion Forensics

CH. RAMESH BABU

Asst. Professor, Dept. Of MCA, K.B.N. College, Vijayawada

***Abstract*— 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. 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 follow 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 that is 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.**

With the birth of the Internet and networks, the computer intrusion has never been as significant as it is now. There are different preventive measures available, such as access control and authentication, to attempt to prevent intruders. Intrusion detection systems (IDS) are developed to detect an intrusion as it occurs, and to execute countermeasures when detected. Intrusion detection (ID) takes over where preventive security fails. In order to choose the best IDS for a given system, one should be aware of the advantages and disadvantages of the each IDS. This paper views a forensic application within the framework of Intrusion Detection and details the advantages and disadvantages of each IDS.

I. INTRODUCTION

In a perfect world the need for determining the activity conducted on a network or within a computer would not be necessary; however, this is not a perfect world and there are times when it is imperative that the activity of a computer be monitored. There should be a way for an individual to observe assets, such a computer or network, in times when possible intrusion or misconduct has occurred. For this reason, computer forensics, a newly developed area of computer science, becomes an increasingly more important aspect daily and will be widely used in the twenty-first century.

The widespread use of computers has caused computer crimes to increase at an alarming rate. Computers have given criminals a new approach to carrying out their misdeeds. After a crime or a questionable act is detected on a computer, a digital investigation must follow. The investigation is used to determine the scope of the problem. The computers investigated will typically be either those used to commit the crime or those which are the targets of the crime.

During the Enron incident a great deal of paper was shredded to avoid leaving evidence of a wrong-doing. However computer forensic investigators were able to recover a large extent of the information in electronic form. In computer forensics, a case may be as simple as to determine whether or not an employee is engaging in improper activity on the network; or it can be as severe as determining where a major attack originated from, such as the SOBIG virus. For these reasons, computer intrusion forensics is an emerging field of essential research.

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. Whereas Intrusion forensics relates to the investigation of attacks or suspicious behavior directed against computers perse. 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.

II. Problem Definition

The field of digital forensics is a relatively new field of study. Many of the techniques used in computer forensics have not been formally defined. Computer Forensics is looked at as part art and part science. Computer Forensics will evolve into a science as more research and standardized procedures are developed.

A survey of the field of computer intrusion forensics will be given in this paper. The goal of this paper is to explain the advantages and disadvantages of computer intrusion forensics. A formal definition of computer forensics will be given. 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. This paper will explain the rights granted to a company who plans to implement such tool and will provide information on tools currently available for use in computer forensics. Last, the paper will explore ways that an intrusion detection system can be used in correspondence with computer forensics.

III. Computer Forensics

s

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. 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.

These are just a few examples of when computer forensics may be used. There are numerous other times when computer forensics can be employed. Computer forensics involves many common investigative techniques used by law enforcement. The only difference is they are used on digital media [Wright 2001]. 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. Great care must be taken in the preservation and recovery of data.

Computer Forensics Methodologies

During a computer forensics investigation there are a variety of steps that must be taken. The following steps, defined in the book Computer Forensics: Incidence Response, form the basis for conducting a forensics investigation. Each of these steps can be further refined.

1. Acquire the Evidence
2. Authenticate the Evidence
3. Analysis the Evidence
4. Present the Evidence

Along with this methodology developed by Kruse II and Heiser, other more formal methodologies have been developed. These methodologies have been established to aid in the proper sequence of actions taken in an investigation. Some of the methodologies are abstract and can be used in any situation which concerns digital evidence and others are aimed at a certain implementation.

The abstract model consists of nine phases "identification, preparation, approach strategy, preservation, collection, examination, analysis, presentation, and returning evidence". The benefit of the abstract model is that it can be used in any situation where digital evidence is involved, not just for examining computers. The disadvantage of using an abstract model is the processes may not be defined as precisely. In some cases when a problem is well defined it may be beneficial to use a non-abstract model.

Data Preservation, Recovery and Examination

The analysis of data in a computer forensics investigation involves three main steps: preserving, recovering and examining data. Recovering data in a computer forensics investigation is a major dilemma. The data that an investigator is looking for can be almost anywhere. It could be on the suspect's computer or in a remote location. A major problem is locating the computer on which the sought-after evidence is located. In a network environment it can be very difficult. Network analysis tools may be needed to help track down the location. Once the computer is located, the hard drive is where the Majority of evidence can be found, but it is not the only place. Some of the places to look for evidence in an investigation are:

- Hard drives
- Memory
- System
- Email servers
- Network traffic

These are just a few places where evidence can be discovered. 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.

IV. Software & Hardware 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.

One of the first things done in an 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.

V. Evaluation and Results

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.

VI. References

[1] Barber, Richard. "The Evolution of Intrusion Detection Systems-The Next Step" Computer & Security, Vol. 20, Issue 2, 1 April 2001, pages 132-145

[2] 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

[3] 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.

[4] Caloyannides, Michael. Computer Forensics and Privacy. Boston, MA: Artech House, 2001.

[5] Crayton, Christopher The Security+ Exam Guide: TestTalker's Guide Series. Hingham, MA: Charles River Media, Inc., 2003.

[6] Department of Justice. "Searching and Seizing Computers and Related Electronic Evidence Issues." Computer Crime and Intellectual Property Section.

[7] 17 Dec 2001 http://www.usdoj.gov/criminal/cybercrime/searching.html (23 Non 2003)

[8] Fisher, Dennis. "Blaster Worm on the Move" eWEEK Enterprise Neand Reviews Online. 12 Aug. 2003http://www.eweek.com/print_article/0, 3048, a=46260, 00.asp (8 Sep 2003)