Computer Intrusion Forensics
Literature Review

Nathan Balon
CIS 544
October 20, 2003

Title

Computer Forensics: Incident Response Essentials by Warren G. Kruse II and Jay G. Heiser

Reviewed by Nathan Balon

Introduction

Computer Forensics: Incident Response Essentials is an introduction to the field of computer forensics. The authors go into detail on a variety of ways to investigate computer crimes. First, the authors describe ways of preserving the data on a computer system. Then, they discuss techniques for examining data on both the Windows and UNIX platform.

Problem

Computer crime is a major problem in any corporation, and the number of such crimes continues to grow. There is a rising need for individuals who are able to investigate and track computer crimes. The problem discussed in the book is how to carry out a digital investigation. Computer Forensics is a relatively new field so there are not many trained professionals in this area. The book **Computer Forensics** gives detailed examples of how an investigation is carried out. Locating evidence of a computer crime is a difficult process. The authors show how to locate evidence on a computer and then carry out a through analysis of the evidence.

Review

The book starts by giving the reader a good understanding of what computer forensics is about. Kruse and Heiser state, "Computer forensics involves the preservation, identification, extraction, documentation, and interpretation of computer data" (2). The authors give three steps to be taken in an investigation. The first is to acquire the evidence. During this stage, computers and hard drives are seized from the suspect. The authors suggest labeling all seized equipment and keeping detail records of the evidence. The second step is to authenticate the evidence. A complete bit level copy of the hard drive should be performed. Then, a hash function such as MD5 should be used on the entire drive. By using the hash function, the evidence can be proven to be authentic. In the third step, the evidence must be analyzed. Various programs and commands can be used to analyze the data that was collected. If enough evidence is found to prove a case, the finding will be presented in court.

The Internet is the primary medium used by attackers to commit computer crimes. A forensics investigator needs to be able to track an attacker on the Internet. The authors show how IP addresses and DNS names can be the starting point for locating an attacker. The utility nslookup can be used to find the IP address and domain names. If the attacker used a dial-up connection, it may be possible to gain information from their ISP. The

ISP's RADIUS server may contain the phone number that an attacker used to establish a connection. Email and newsgroups also can be used to track individuals on the Internet. Email can be used to gather evidence for a case. One problem with email is that it can not be authenticated. Because it is relatively easy to spoof an email address, the email may not come from who it says. The email header contains some valuable information that can be used to track the source of the email. SMPT server logs can also be used to gather further information. Intrusion Detection Systems (IDS) can be used to tell when an attack is underway. An IDS can also be used to gather forensics' information. IDS's keep extensive log files that can be analyzed.

The majority of data that will be analyzed in an investigation is contained in the hard drive. The first thing that should be done when analyzing a hard drive is to find out partition information. The number of partitions on a drive and the file system used should be established. Data can be found on a drive in many different places in files, slack space, unallocated blocks, unused partitions and the boot track. It is hard to permanently erase data on a hard drive. Formatting the drive still leaves the data on it. Tools such as a hex editor can be used to find deleted files on a hard drive that have not yet been overwritten. Even when data is overwritten on a drive, there are still traces of the previous data. So it is possible to recover data that has been overwritten - provided enough time and money is allotted. The authors show that there are traces of data on a drive even when it is overwritten seven times.

Many techniques can be used to hide data. A forensics investigator needs to know how to retrieve this hidden data. Experienced criminals will go to great lengths to cover their tracks and make it hard to recover data. Some of the techniques that can be used to hide data are encryption, compression, steganography, and creating codes. Files can also be hidden by placing them in obscure locations, creating names that look like legitimate files, storing them in remote locations and using invisible names. Recovering files may also involve the need for cracking passwords. There are many password cracking programs that can be used. For example, LophtCrack, is used to crack Windows NT passwords. Finding evidence in files is a tedious and long process, but it is where the evidence will most likely show up.

Hostile code is used by hackers to gain and maintain control of a system. One way a hacker can gain access to a system is by using sniffing tools to try to capture passwords of users. Another technique frequently used to gain access is to scan a system for known vulnerabilities. Once a hacker gains access to the system they usually hide a malicious code that allows them to re-enter the system with out being detected. A system in question should be examined for a malicious code. The authors recommend not to use the actual computer in question while looking for the malicious code, but to use a known uninfected computer to scan for the code.

A computer forensics investigator should have a wide range of tools to help in an investigation. First, the investigator should have hard drive tools to find out information about the number of partitions and file systems used on a computer. The authors recommend using Partition Magic. Next, various types of file viewers can come in handy

for viewing unknown file types. Quick View Plus is a program that supports over 200 file types that can be used. Also, searching through large amounts of text can provide many clues in an investigation. The authors suggest using dtSearch for finding key words in text. Furthermore, 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. Finally, a wide range of programs made especially for forensics investigations are available, such as ForensiX and EnCase. A forensics investigator should be familiar with many of these different programs to aid in an investigation.

The two operating systems that are most often examined are UNIX and Windows. The authors conclude the book by showing various issues that are specific to these operating systems. An investigator may have to base the approach taken upon what operating system is used. Each operating system has it own utilities that can be used in an investigation. The Windows registry contains a wealth of information that can be discovered. A non-technical user may not cover all of the tracks in the registry. UNIX is the most popular system used to carry out attacks because of the power of its command line. A computer forensics investigator can expect to examine many UNIX systems. On a UNIX system, if a hacker gains the root account he can replace shared libraries and disguise programs. One technique used to discover changes in shared libraries is comparing their hash values. Also, an inexperienced hacker may leave evidence in the log files. In both Windows and UNIX, there are many things an investigator can do to gather evidence.

Discussion

The book **Computer Forensics: Incident Response Essential** is a very informative book. It is geared towards those who have a strong background in computers but have limited knowledge of computer forensics. The authors give many different programs that can be used in a forensics investigation to get the reader started in the field. They also give many illustrations of these programs in actual use. The most interesting chapter in the book dealt with hard drive recovery. If someone is interested in getting into the field of computer forensics this is a good book with which to start .

References

Kruse II. Warren G. and Heiser. Jay G. **Computer Forensics Incident Response Essentials**. Reading, MA.: Addison-Wesley, 2002.

Title

"*High-tech Holmes*" by Jon Wright

Reviewed by Nathan Balon

Introduction

Computer crimes are much like ordinary crimes. The same techniques used to investigate physical crimes can be used to investigate cyber crimes. The only difference is that an investigator is searching for bits and bytes instead of DNA.

Problem

The paper by Jon Wright discusses how to conduct a criminal investigation using digital evidence.

Review

Computer forensics investigators conduct their investigations in a manner similar to that used by normal forensics investigators. The only real difference between the two is the medium and tools used. The same basic principles apply to both kinds of investigations. The article "*High-tech Holmes*" covers four subject areas in a computer forensics investigation. A computer forensics investigator must first preserve evidence, then analyze the evidence, and last come up with their findings.

Once a questionable activity has taken place the first thing that must be done is to preserve the evidence. This is a very important step in an investigation. If the evidence becomes altered it may be harder to have a case that will stand up in court. First, a complete bit copy should be done to the media to preserve the integrity of the original data. Special programs can be used that keep the integrity of the data intact. The data should be copied to a read only device such as a CD-ROM so that time stamps of files will not be modified.

Analyzing the data is the next step in the investigation. During this step, the investigator is looking for certain incriminating evidence. The author, Jon Wright states that there are three different places where evidence can be found. They are: logically accessible data, deleted files, and unallocated space. Each of these different places requires a different form of investigation. First, logical files are usually the easiest to recover. Wright suggests looking for files with changed names and extensions while examining the logical data. Also, the potential problem of finding encrypted files may present itself. It is usually easier to find an unencrypted version of the file somewhere on the medium then actually trying to break the encryption. Password protected files are usually easily broken by password cracking programs. Second, deleted files can be recovered from a hard drive. The operating system deletes pointers to the files, but it does not actually delete them from the medium. Unless these files are over-written, they will still reside on

the disk. A forensics investigator is then able to recover these files. Third, unallocated space can be used to recover information for an investigation. This area is used for cache and temp files by programs and the operating system. Investigators can look here to find clues that are not available in the other two sections. By examining the unallocated space of the drive, it may be possible to recover email messages that were received or composed on a system.

After the data has been analyzed, the investigator must present their findings. If a criminal activity is found to have taken place the investigator must be prepared for court. The findings should be well documented and easily explained to a jury. A formal report should be prepared. The forensic investigator should be as professional in preparing their finding as he was in the original investigation.

Discussion

In the article, Wright discusses how to conduct an investigation into a computer crime. The main focus of the paper is to show how to protect and analyze digital evidence. The same care must be placed in conducting a digital investigation as a physical investigation. The same principles apply to either case. The only real difference between the two is the tools used to conduct the investigation.

References

Wright. Jon. "High-tech Holmes". Security Management. Arlington: July 2001. Vol. 45, Issue 7; pg. 44, 6 pgs

Title

"*Linkin' Logs to Fraud*" by John J. Melina Jr.

Reviewed by Nathan Balon

Introduction

Computer logs are a valuable resource in conducting a computer forensics investigation. A thorough examination of the system logs can turn up a great deal of evidence. It is even possible to conduct an investigation by solely using the system log files.

Problem

In computer forensics much attention is placed on a user's computer. Specifically, the majority of the focus is on the computer's hard drive that was used to commit a crime. Using only the computer in question to conduct an investigation can lead to insufficient evidence to be gathered, which can result in lack of a conviction. System log files contain a great deal of information that is often overlooked.

Review

The article is written to show the importance of using the log files when conducting an investigation. Computer logs can make the difference between a strong and weak case. The majority of events that take place in a computer system are recoded in log files. The author states, "that law enforcement will typically seize computers but will not take the system logs." (2) 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. By examing the logs, it can be proved which user account actually performed the questionable act.

The structure of the computer system is the first thing that must be examined before conducting an investigation. The author states, "An investigator must gain a basic understanding of the subject organizations IT architecture, its enterprise network infrastructure and the general components of the computing environment, including the information security controls in place." (2) By gaining a basic understanding of the system, a more thorough investigation will follow. The author emphasizes not collect evidence only on the computer in question but also on the server and the network connecting the two.

An investigator should collect as much evidence as possible, when an incident occurs. There are a great amount of log files that are kept in an information system. Logs are also kept by many devices in a system. The author suggests collecting information from as many logs as possible. Servers have authentication logs that tell who and when accessed the server. Firewalls and Intrusion Detection Systems have logs that can be

evaluated for suspicious activities. Many network routers also have logs that can be examined to reconstruct evidence. Many application keep there own log files such as email. Each of these logs should be evaluated and they can help reconstruct a questionable incident. Author states when discrepancies between logs occur there is a high likelihood that someone tried to modify one of the logs to cover their tracks.

The author also gives an example of a crime that occurred at a bank. The case was never prosecuted because of lack of evidence. If during the investigation, the logs would have been seized, it would have been able to reconstruct the entire crime from the log files.

Discussion

Log files can be an excellent aid in help to determine what actually took place in a forensics investigation. If a company logs most of there event and keeps the log files it may be possible to recreate what actual took place in the event in question. The only problem that could occur is if the organization does not maintain the logs for long period of time.

References

Melia. John. "Linkin' Logs to Fraud". Security Management. Arlington: Nov. 2002 Vol 46. Issue 11; pg. 46, 6 pgs