Digital forensics investigation critical thinking example

Law, Evidence

SOURCES OF EVIDENCE IN DIGITAL FORENSICS INVESTIGATION

ABSTRACT

Today’s society is becoming, increasingly, interconnected through the use of networking technologies and the proliferation of internet. As such, computer intrusions and security incidence are on the increase. Organizations and companies find the use of internet unavoidable in order to advance their operations and efficiency. The ability to handle computer security concerns resulting from seamless connectivity proves to be a major challenge. Other insecurity concerns resulting from insider file alteration and malware installations are equally harmful and should be treated with utmost considerations. As a result, the field of digital forensic investigation has risen to help in unearthing such incidences. This paper is going to focus on four sources of data that a forensic investigator will rely on in respect to network intrusion, malware installation and insider file deletion.

Forensic preparedness is crucial for any digital investigation in respect to responding to a critical incident. The detection of an intrusion forms the basis for a digital investigation and subsequent decision making in haste. When intrusions are detected, normally inadvertently, speedy and accurate response is necessary. This is in order to determine the source and the extent of intrusion protect sensitive and confidential data. Also, this is to protect the systems and networks and ensure their continued operation. More importantly, the ability to collect evidence in the form of data of what transpired and in a manner consistent with the legal provisions is crucial in dealing with the intrusion. The data collected can be used to sustain a case

at the law of courts or conduct disciplinary actions against insiders.

Once an intrusion has been detected, a number of techniques can be used for network monitoring. The network can be shut down to disconnect the intruder from doing more damage or the network can be left open for more monitoring and tracing of the intruder. The intruder is pursued by gathering more information through covert monitoring of network traffic and file access functionalities. The monitoring leads to a determination of compromised data in the system realized through irregular patterns.

Intrusion detection methods can be manual or network based. Manual detection methods seek to find modifications that have altered state of files and Meta data.

SYSTEM LOGS AND FILES

The knowledge of, and the ability to, competently differentiate the state of a network will lead to crucial evidence of an intrusion. For instance, network signature recognition and system anomaly behavior reveal considerable evidence about an intrusion event. The application of manual intrusion detection and digital investigation methods reveal modifications or anomalous system logs, process files and transaction records. Evidence of modification is obtained when the system files and utilities hash are compared against the expected hash. A library of expected hashes is kept for general reference, and when the expected hashes differ from the expected database, it is inferred that there was a modification.

A log file is an automatically generated record of past activity in a computer system usually organized as a sequence of entries. Its components include timestamps and reason for generating the entry. A computer system will

contain numerous logs some of which are created and maintained by the different applications and the operating system.

Logs are generated when a significant activity happens in a computer system. For instance, a single TCP wrapper activity occurs when a TCP connection is initiated, and another one is recorded when the connection is disconnected. Log files, therefore, forms an essential component of a digital investigation in that their analysis informs the forensic experts of a record of happenings. The presence of two log file entries supporting the initiation and termination of a TCP wrapper for a certain connection informs the forensic scientist of some connection that indicates the time of happening. This is possible with the exception that the entries have not been tampered with in a forgery process. To ascertain the validity of the evidence, more corroborating evidence in the form of timestamps is used to determine the temporal order of entries. By so doing, it is possible to determine if the log entries were recorded on different computer systems with dissimilar system clocks. Each stamp clock impression and skew will give an estimation of which log was generated after the other. Likewise, a coarse resolution of the clocks may reveal identical timestamps, which may imply that the logs were generated at different intervals.

Apart from the log files, file system objects subjected to reconstruction processes may reveal evidence of intrusion. Operating systems is characterized with storage devices represented by equally spaced storage blocks known as clusters. These clusters can be read and written independently and the file system allocates a different cluster for storing user data and another for storing structural data.

Structural information includes such objects as directory tree, file names, location of data blocks utilized for individual files and location of unallocated clusters. Operating systems manage the structural information in such a manner that they can be utilized, for event reconstruction to show a record of happenings in a system. System logs recording suspicious behavior is the most crucial component of digital evidence as they detail intrusion attempts and the system behaviors prior to and after the attack. System logs play a crucial role in the process of collecting digital evidence and must be treated as such. Some systems have different types of logging in their default configurations while others do not. For example, trusted operating systems such as those used by national security agencies have advanced system logs. These logs provide a high degree of detail with distinct precision. In a digital investigation exercise, the types of logs and logging procedures in place provide evidence of file access logs, network logs, application logs, process logs and logs.

COPIED AND DELETED FILES

In most forensic investigation methods, there are traces of evidence that imply the compromise of a system. These traces are mostly left behind after the actions of malicious intruders. Methods have been developed to determine the data that was copied or deleted from a computer system stochastic forensics. This is one such method that determines the data that have been stolen through randomly determined patterns. The research on stochastic forensics revealed that about 90% of data on a computer system are not usually utilized.

As per , the routine of data usage provides revealing information of an

attempted or executed copying or deletion of data. A long tailed pattern signifying the use of few objects reveals a meticulous graph which is broken when copying is carried out. Copying process involve an abrupt entry and exit of the system with an unusual pattern. This signifies change of patterns of execution and most probably an intruder activity. This mechanism is used to reconstruct an unusual pattern of access even after a lengthy period. In this incidence, files, which are normally not accessed, are copied en masse. The technique considers a programmatic inquest of the directories and subdirectories with particular focus on the timestamps of access to detect random behaviors. An application of such evidence is the case of intellectual theft.

Individual files have all their information stored in standardized files entries whose structure and organization contrast the file system structure. In Windows, for instance, information of a file is located in an entry of the Master File Table. At the first instance of neither disk partition nor formatting, all the standardized file entries are set to unallocated value. A file entry that is allocated to a file activates its filling of the field with the proper information about the file.

In most file systems, the file entry is not modified to unallocated once its contents are deleted from the entry. As such, the presence of file entries without matching “ unallocated” value implies deletion of a file entry. It shows that there was an existence of a file entry which has been subsequently deleted, thus presenting relevant evidence to investigators. Analysis of files system will result i9n more evidence about their names, access permissions, timestamps, and their locations of allocated disk blocks.

This information always changes when a file is manipulated by the operating system calls.

Through equivalent steps used to analyze log files, file attributes can be analyzed with timestamps providing relevant details for event reconstruction. NTFS files have three timestamps I their active mode. These include time of time of creation, time of last access, and last modification. Tools available in the computer systems analyses the MAC times of both active and deleted files and compares them with the log file. The log files records the corresponding operation (MAC) of each file entry with the corresponding timestamp. Likewise, signatures of the activities in a computer system can be identified in MAC-times through a host of practices. For example, the restoration of a directory from a backup system can be detected by different time stamps on the directory and subdirectory. The signatures of deleting, running and compiling a program is explored and included when a delete, compile and run exercise is executed. The traces of the deleted programs source code; executable files and compiler temporary files are traced and used evidence.

A “ move file” activity result in deletion of an old entry and the creation of a new one in Microsoft FAT file system. The new file system retains the same block location as the old one and in that matter, the revelation of a deleted file entry with the same features as the active file implies the possibility of moving a file.

INTRUDER ARTIFACTS

Intruders leave behind numerous and different forms of files on the compromised system ranging from stolen password files, source codes,

programs, and sniffer log files and exploit scripts. Others will leave processes and applications running in memory. Such evidence in the form of programs is referred to as remnant files while source code and malicious scripts are called artifacts.

According to , malware intrusions replace the system file systems with different file systems having the same names but different functions. They offer a method of concealing their actions on a system thereby presenting a source of evidence for a digital investigation process. Because these malicious programs are presented with original namesake except their content, they are hard to detect and require proper cryptographic methods to unearth them. A complete read only list of the checksums of system files is conducted to determine artifacts from the original file systems. Recovered artifacts are analyzed and documented for comparison with the suspects computer systems. A useful scenario is where a warrant of arrest is issued. After the issuance, the law enforcers supply the victim with a copy of the seized code to be compared with the artifacts recovered from the victim’s site. Artifacts are best analyzed on isolated system, and care is taken to capture the copy of the artifacts and the surrounding to, possibly, mirror the original environment. Intrusion detection tools are classified into two; host intrusion detection and network intrusion detection systems. The principal roles of these tools are to provide round the clock monitoring and communication systems that detect, alert and block suspicious traffic on a critical network.

Host intrusion detection systems are security methods used in computers and network management. In HIDS, anti-threat applications such as spyware-

detection programs, antivirus software’s and firewalls are installed on every networks computer. This is applicable in two-way access platforms such as the internet and gathers information from various sources and analyses it to identify possible areas of attacks. HIDS is, therefore, suitable for business critical hosts and servers in a DMZ that are compromised more frequently. HIDS operates by utilizing a number of variables on the host system namely; CPU usage, system processes, file access and integrity checking and registry entries among others. Thus, it has the capability to utilize system properties such as logs, system services and registry events for detection and analysis. However, it has a disadvantage of utilizing much of the system resources since it runs on the host. In addition, by the time the HIDS systems detects an attack, the damage is already done.

Conclusion

In conclusion, the covered sources of evidence for a forensic investigation are crucial for sustaining court cases and preventing future attacks. If the evidence lacks the integrity it deserves, it cannot be used for the intended purpose and, as a result, lead to considerable losses.

References

Bace, R. (2009). Vulnerability assessment: Computer Security Handbook . John Wiley & Sons.

Brian Caswell, J. B. (2008). Snort 2. 1 Intrusion Detection, Second Edition. Syngress.

Cameron H. Malin, E. C. (2008). Malware Forensics: Investigating and Analyzing Malicious Code. Syngress.

Ciampa, M. D. (2011). Security+ Guide to Network Security Fundamentals.

Cengage Learning.

Glenn R. Lowry, R. L. (2007). Information systems and technology education. Idea Group Inc .

Kim, S. F.-h. (2007). IT Security Review: Privacy, Protection, Access Control, Assurance and System Security. International Journal of Multimedia and Ubiquitous Engineering, Vol. 2 No. 2 .

Kizza, J. M. (2009). A guide to computer network security. Springer.