ISSN:2320-0790

COMPUSOFT
An International Journal of Advanced Computer Technology

Audit Planning for Investigating Cyber Crimes

Dr. Ajeet Singh Poonia

Associate Professor, Department of CSE, Govt. College of Engineering and Technology, Bikaner, India

Abstract: The exponential growth of technology into many aspects of everyday life has led to development of the modern concept of information society. This development of the information society offers great opportunities which are accompanied by new threats. Attacks against information infrastructure, Internet services, online fraud and hacking attacks are just some examples of cyber crimes that are committed on a large scale every day and the financial damage caused by cybercrime is enormous. The risks of cyber crime are very real and too threatening to be ignored. Every franchisor and licensor, indeed every business owner, Internet service providers, domain name registries, universities, law enforcement agencies, and other cross-industry stakeholders has to face up to their vulnerability and do something about it. An organized effort toward fighting cyber crime is required. In this paper, an effort has been done in this direction.

Keywords: Information Society, Internet Services, Online Frauds, Hacking, Cyber Crime, Vulnerability.

I. INTRODUCTION

In today's world cyber crime is increasing rapidly with the growth of technology. Wide range of cyber crimes are prevailing in the society today. Cyber crime has become a new subject for researchers. Lot of research is going on and endless has to be go because the invention of new technology leads to the technical crime. Solution of each case requires a very complicated task. Presently the digital investigation process has been directed by technology being investigated and the available tools. The infrastructure to investigate cyber and electronic crimes is based on the prevailing cyber and electronic laws. Many digital forensics practitioners simply follow technical procedures and forget about the actual purpose and core concept of digital forensic investigation.

II. CYBER CRIME

A generalized definition of cyber crime may be "Unlawful acts wherein the computer is either a tool or target or both" [1]. Cyber Criminal is a person who commits an illegal act with a guilty intention or commits a crime in context to cyber crime. Cyber criminal can be motivated criminals, organised hackers, organised hackers, discontented employees, cyber terrorists. Cyber crime can include everything from non-delivery of goods or services and computer intrusions (hacking) to intellectual property rights abuses, economic espionage (theft of trade secrets), online extortion, international money laundering, identity theft, and a growing list of other Internet-facilitated offenses. Further, it is not easy to identify immediately about the crime method used, and to answer questions like where and when it was done. The anonymity of the Internet makes it an ideal channel and instrument for many organized crime activities[2].

III. CYBER CRIME INVESTIGATION

"We have probably heard the saying "information is power," and that is certainly true when a cyber crime is committed. But the right information can also empower us to protect him from being caught up in the blooming industry that is cybercrime". There are various methods, models, steps and different mechanism to investigate the cyber crime. Some of the basic steps of standard cyber crime investigation model are Realization, Authorization, Audit Planning, Auditing, Managing digital evidences, Hypothesis, Challenge Analysis and Report Abstraction and Dissemination [3]. Among all these steps/phases Audit Planning plays an important role among all , as the basic concept behind the auditing is to extract/discover the data and then match/recognize the piece of digital evidence.

IV. AUDIT PANNING

Auditing Planning is the most important phase of cyber crime investigation procedure. The result of this phase is the actual 'cause' and the area affected by the cyber crime. The basic concept behind the auditing is to extract/discover the data and then match/recognize the piece of digital evidence. In the audit phase, the investigating team may take help from the references, records etc. available from the reports of previous such cases taken place in the organization itself or outside the organization. Initially the auditor focuses on reviewing the answers the client gave to the questions in Audit planning phase. Figure 1.1shows the Use Case Model of Auditing [3]

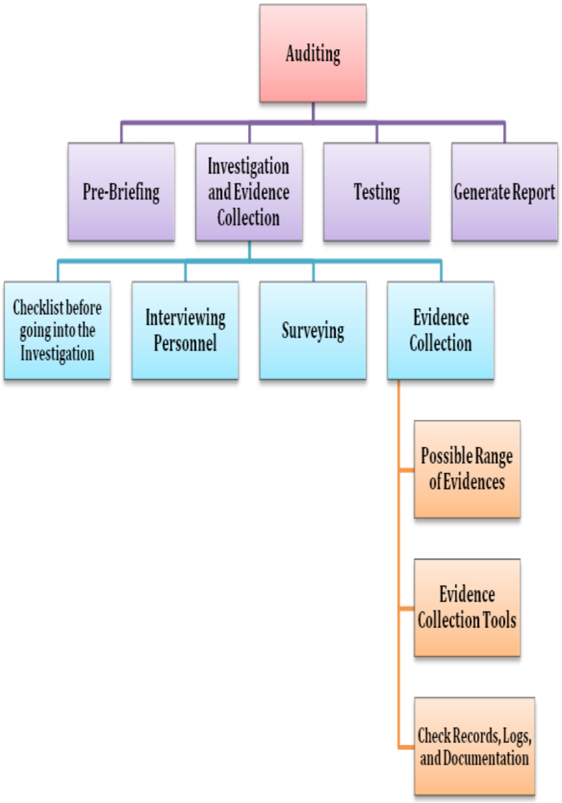
Auditing
Pre-Briefing
Investigation and Evidence Collection
Testing
Generate Report
Checklist before going into the Investigation
Interviewing Personnel
Surveying
Evidence Collection
Possible Range of Evidences
Evidence Collection Tools
Check Records, Logs, and Documentation

Figure 1.1 shows the sub-phases of Auditing Phase

1. PRE-BRIEFING

The first thing to do at the client's site is to go through a pre-briefing. This is about a 15-minute period in which auditing team interfaces with the client and the personnel, the client has gathered to help in its investigation, giving the team the opportunity to ask some additional questions, meet key personnel of the organization (managers, system administrators, key project personnel who used the compromised system, security personnel, etc.), and obtain an update on the situation.

2. INVESTIGATION AND EVIDENCE COLLECTION

Basically Investigation can be as simple as finding the computer used by a suspect and confirming that it is the one of interest to the investigators and it could be as complex as tracing computers through multiple ISPs and possibly in other countries based on knowledge of an IP address .Investigation totally depends on the gravity of crime actually held.

2.1 CHECKLIST BEFORE GOING INTO THE INVESTIGATION

Before going for the investigation, the investigator/auditor should follow the basic steps so that the investigation goes in a right direction with a fruitful output. The steps are:-

A. Sanitize your evidence storage devices by wiping them at the physical level and then partitioning and installing the appropriate file system.

B. Observe and record the physical characteristics of the digital evidence (location, cabling, peripherals, and status).

C. If necessary, use trusted software tools to collect volatile information (memory contents, network connections, etc.).

D. Disconnect the computer from any network connection (modem, Ethernet, wireless).

E. If the computer is powered on, note what is displayed on the screen (a digital camera is required here).

F. Power off the computer by pulling the power cable from the computer.

G. Attach the appropriate digital storage device to either the imaging computer/device or the subject's computer.

H. Copy the evidence image to a backup storage device before performing any analysis, and store the original evidence image in a controlled evidence storage facility.

I. Create and maintain the appropriate documentation.

2.2 INTERVIEWING PERSONNEL

Interviewing plays an important role in the investigation part. Through interviewing investigator/auditor comes to an idea of the actual scenario of the crime held and can conclude to a certain point.

2.3 SURVEYING

The survey phase finds the obvious pieces of digital evidence for the given type of crime. It determines what a particular piece of digital evidence is, and identifies possible sources of data, for e.g. in case of child pornography the investigator would collect all of the graphic images on the system and identify those that could be used as evidence.

2.4 EVIDENCE COLLECTION

Evidence Collection is the important sub phase as compare to other one, as the errors or poor practices at this stage may leads to evidence useless. This is all because that digital evidence is delicate and can easily be lost, i.e. it can change with usage, it can be maliciously and deliberately destroyed or altered, it can be altered due to improper handling and storage. For these reasons, evidence should be expeditiously retrieved and preserved. Also consider that when investigating offences' involving the Internet, time, date, and time zone information may prove to be very important. Server and computer clocks may not be accurate or set to the local time zone. The investigator should seek other information to confirm the accuracy of time and date stamps.

2.4.1 POSSIBLE RANGE OF EVIDENCES

There are numerous resources through which the evidences can be collected for investigation of the cyber crime held. Below mentioned are some of the sources but not limit too [3].

A. Hardware such as routers, firewalls, servers, clients, portables, and embedded devices.

B. Software such as ERP packages for employee records and activities (e.g. in case of identity theft), system and management files. Monitoring software such as Intrusion Detection Software, packet sniffers, keyboard loggers, and content checker.

C. Other sources, such as CCTV, door access records, phone logs, PABX data, telco records and network records, call centre logs or monitored phone calls, and recorded messages.

D. Back-ups and archives, for example, laptops and desktops.

E. Files those are either contraband or illegally possessed. Configuration files showing server or user information, connection history, shared drives on a network, or Internet sites that provide offsite data storage space

F. Data files showing file sharing locations with user names, passwords, search terms, file listings, and date and time information.

G. Log files that show transfers and network activity. Dynamic Host Configuration Protocol (DHCP), and RADIUS logs, which may assist in connecting the suspect to the illegal activity.

2.4.2 EVIDENCE COLLECTION TOOLS

Numerous tools are available in the system for collecting the evidences. Many tools have common features but they all have their own characteristics. Utility of the tools vary from case to case. Below mentioned are some of the evidence tools which are basically used in general.

a) Safe Back

First step at a client site is to obtain a bitstream backup of the compromised systems. A bitstream backup is different from the regular copy operation. When performing a bitstream backup of a hard drive, you are obtaining a bit-by-bit copy of the hard drive, not just files. Every bit that is on the hard drive is transferred to your backup medium. During a copy operation, you are merely copying files from one medium to another. Hidden data exists on your hard drive means that more is present in the hard drive than just the file names you see [4].

b) Get Time

GetTime is used to document the time and date settings of a victim computer system by reading the system date/time from CMOS. Compare the date/time from CMOS to the actual current time [4].

c) FileList, FileCnvt

Now that you have restored your bit stream backup to drive C of your analysis computer, use File List to catalogue the contents of the disk. FileCnvt and Excel are used to properly read the output of the FileList program. Using FileList, it is simple to review the chronology of usage on a computer hard drive, several computer hard drives, or a collection of diskettes [4].

d) GetFree

Now we want to obtain the content of all unallocated space (deleted files) on drive C of your analysis computer and place this data in a single file. This single file can be placed on a diskette or on any media. Any files that were deleted from drive C can be obtained in a single file by this utility [4].

e) Temporary Files

When working with a Microsoft Windows operating system, it copies the Windows temporary files to your Zip Drive D. These files have a .tmp extension.

f) CRCMD5

CRCMD5 calculates a CRC-32 checksum for a DOS file or group of files and a 128-bit MD5 digest. The purpose of having the CRC checksum and MD5 digest is to verify the integrity of a file or files. For instance, once you have collected a file for evidence, run CRCMD5 on it to obtain the CRC checksum and MD5 digest. As long as the file contents are not changed, these values remain unchanged. If they do change, then the integrity of the file has been compromised, and the file may no longer be admissible in a court of law [4].

g) DiskSig

DiskSig is used to compute a CRC checksum and MD5 digest for an entire hard drive. The checksum and digest include all data on the drive, including erased and unused areas. By default, the boot sector of the hard drive is not included in this computation. Similar to CRCMD5, the purpose of DiskSig is to verify the integrity of a hard drive. Running DiskSig on a hard drive held for evidence provides a CRC checksum and MD5 digest. If the hard drive data is altered in any way, the values of the CRC and MD5 will change [4].

2.4.3 CHECK RECORDS, LOGS AND DOCUMENTATION

They are an electronically generated and stored file of information about activities occurring in a system. They are usually in the form of a series of entries each containing descriptive attributes about a past event. Logs provide factual material which assist in the reconstruction of events, such as cyber attacks. There are many different types of logs. For example General logs, such as access logs, printer logs, web traffic, internal network logs, Internet traffic, database transactions, and commercial transactions; every application and operating system on every device on a network may be logged. Logs have been described as the “digital witnesses to transactions between computers and humans.” Unlike human eyewitnesses, logs do not contain human statements which may suffer from bias, prejudice or faulty human recollection. There is an assumption that computer logs are more likely to be accurate as to their content, provided that the logs are authentic and reliable.

3. TESTING

After examining the evidences a test or various test are performed, testing is done experimentally to ensure that the evidences collected are correct or not and the investigation is going on in correct direction or not. If it is found satisfactory, it is eventually tested with past data, experiences, references, data or cases from the current system.

4. GENERATE REPORT

A report containing information about the initial evidences, filtered evidences, crime scene, various investigation reports, crime system and the statements of the witnesses are documented. In this way, the evidence report is a document of importance that is essentially used in further phase of investigation. The goal is to capture as much information as possible so that the layout and important details of the crime scene are preserved and recorded. This report works as a guide for making hypothesis and for drawing the conclusion for the case. The report should be in such a manner that it works as a helping hand for the solution of the case rather than making it a complex one i.e. the report should be easy to understand, technical accordingly, logical, and helpful as a reference for other similar case.

V. CONCLUSION

In audit planning all the necessary preparations are done before reaching the location of crime, by any of the mode or medium. The basic concept behind the auditing is to extract/discover the data and then match/recognize the piece of digital evidence.

VI. REFERENCES

[1] Roshan, N., What is cyber Crime. Asian School of Cyber Law, 2008: Access at -http://www.http://www.asclonline.com/index.php?title=Rohas_Nagpal,

[2] Govil, J., Ramifications of Cyber Crime and Suggestive Preventive Measures, in International Conference on Electro/Information Technology, 2007 IEEE. 2007: Chicago, IL. p. 610-615.

[3] Poonia. A.S et Al., Ph.D Thesis, “Investigation and Precevtion of Cyber Crime in Context to India”, 2013

[4] B.Middleton (2006) Cyber Crime Investigator’s Field Guide