International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 3 Issue 12, December-2014, pp: (16-20), Impact Factor: 1.252, Available online at: www.erpublications.com

Audit Tools for Cyber Crime Investigation

Dr. Ajeet Singh Poonia
Associate Professor, Department of Computer Science and Engineering,
Govt. College of Engineering and Technology, Bikaner, India

Abstract: In current scenario cyber crime is increasing very fast as the technology is growing very rapidly. So the cyber crime investigation is becoming a very complicated task to do without a proper framework. There is wide range of different types of cyber crime today. Solution of each case requires a very complicated task. The digital revolution has created the need of new laws, digital investigators, forensic methods, forensic tools and techniques, to enable the digital evidence presentable in court of law. To date, the digital investigation process has been directed by technology being investigated and the available tools. In this research paper, vari ous technical and doc umentati on tools are analyzed and disc ussed which are used in Cyber Crime Investigation.

Keywords: Cyber Crime, Cyber Crime Investigation, D igital investigators, Forensic methods, Forensic tools.

Introduction

Computer is an imperative part and plays an important role in cyber crime whether it is stand alone or on network. Basically it can be categorized in three different categories, firstly Computers as a Target where the computer is used to destroy or obtain information. In other words, the computer itself is the target. Such offenses include theft of intellectual property, marketing information, blackmailing etc [1], Secondly Computer Vulnerability where computer crime classifies computer crimes in terms of vulnerability falling into six types: Hardware, Software, Networks, Information/Data, Computer-controlled devices, and Physical structures and buildings [2] and thirdly Computer as a source of Threat where computer crimes fall into two groups: Insiders and Outsiders. Insiders are the people working for an organization like Network administrators, system operators, application programmers, or end-users. They have the best opportunities to commit crime. Outsiders are the not working in organization. They commit the crime by using electronic bulletin boards, networks, internet, or telecommunication media. Such people are known as hackers, or crackers. They attack systems from the outside, most likely from a basic home computer [3].

Cyber Crime

Globalization and digital convergence in the emerging knowledge society has raised complex ethical, legal and societal issues with some complex questions on the freedom of expression, access to information, the right to privacy, intellectual property rights, digital divide, cyber crimes, digital security and privacy which has led to the growth of new forms of national and transnational crimes which have virtually no boundaries and may affect any country across the globe, which have affected human lives directly or indirectly. Among all cyber crime is a burning issues in today's scenario.

In cyber crime computer is used as a tool in the following kinds of activity- financial crimes, sale of illegal articles, pornography, online gaming, intellectual property crime, e-mail spoofing, forgery, cyber defamation, cyber stalking. The computer may however be target for illegal acts in the following cases- unauthorized access to computer/ computer system/ computer networks, theft of information contained in the electronic form, e-mail bombing, data didling, salami attacks, logic bombs, Trojan attacks, internet time thefts, web jacking, theft of computer system, physically damaging the computer system[4].

Audit Planning for Cyber Crime Investigation

In cyber crime investigation the audit planning is done where all the necessary preparations are done before reaching the location of crime, by any of the mode or medium. In such preparations, the auditing team gathers all sorts of queries that need to be put to the organization/person in order to get maximum information about the background of the system suffering from crime and about the crime itself. Here the investigation team tries to plan a systematic audit that could find out or detect what wrong actually went with the organizational network or communication system and what could be the possible reasons facilitating cyber crime. The team plans the steps to reach the actual reason for the happening of the cyber

crime. This is basically a planning or preparation phase so the auditing team prepares all the tools that it is going to use for auditing. In any case the planning part is influenced by information from both internal and external of the investigating organization/system. From outside, the plans will be affected by regulations and legislation and other external sources, which set the general context of the investigation and which are not under the control of the investigators. From internal of the organization/system, there will be the organization's own strategies, policies, and information about previous investigations, if any. The planning activity may give rise to a need to backtrack and obtain further authorization.

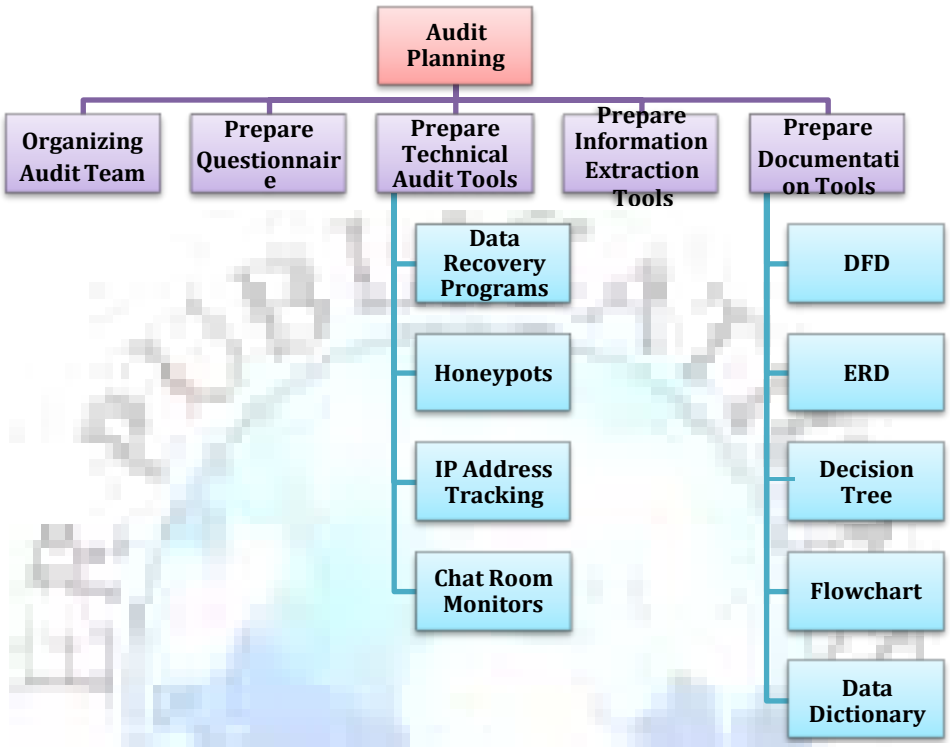

Figure 1.1 shows the sub-phases of the audit planning phases

Technical Audit Tools for Cyber Crime Investigation

The technical audit is meant for gathering all the information about the system which is affected by the cyber crime. The technical audit tools are gathered from the repository depending upon the type of cyber crime taken place. These tools may be used for mapping responses of the person providing information with the evidences collected. Moreover tools for recording the statements of the witnesses are also prepared. Tools should be according to the case, can vary from person to person, organization to organization. Tools can be for technical, logical or experimental case. They can also be according to the case happened, internal or external part of the organization. The Audit tools are basically Data Recovery Programs, Honey pots, IP Address Tracking, Chat Room Monitors, log files etc. These tools help the law enforcement agencies in investigating the growing type of crime and identify the individuals committing it. Some of the basic audit tools that generally works as a base tool and are used in any type of cyber crime held, are discussed below.

A. Data Recovery Programs [4, 5].

These are the software's used to extract information from a computer's hard drive after it has been erased or damaged. Not all data will be recoverable. Retrieval is only done on the availability of the drive. These software's are used to recover files that a suspect may have tried to remove, such as evidence of child pornography. The quality of the files retrieved depends on certain factors, like what method was used to delete the files and the physical state of the hard drive itself.

Some examples are:-

- Knoppix: The original Linux Live CD. It contains many useful utilities for data recovery. It can be used to copy files easily from hard drives with inaccessible operating systems. To quickly and more safely use Linux software, the Live CD can be used instead of installing another Operating System [6].

- SpinRite: It is a software program for scanning magnetic data storage devices such as hard disks, recovering data from them and refreshing their surfaces [7].
- SystemRescueCD: It is an operating system for the x 86 computer platforms, whose primary purpose is to repair unbootable or otherwise damaged computer systems after a system crash. SystemRescueCD is not intended to be used as a permanent operating system [8].
- Trinity Rescue Kit: It is a free command-line Live CD Linux distribution created especially for rescuing Windows PCs. It is aimed specifically at offline operations for Windows and Linux systems such as rescue, repair, password resets and disk cloning [9].
- Consistency checkers

❖ CHKDSK: A consistency checker for DOS and Windows systems [10].

❖ Fsck: The system utility fsck (for "file system check") is a tool for checking the consistency of a file system in Unix and Unix-like operating systems [11].

❖ Disk First Aid: A consistency checker for Mac OS 9 [12].

❖ Disk Utility: A consistency checker for Mac OS X [13].

- File recovery

❖ CDRoller and IsoBuster: Recovers data from optical discs [14].

❖ dvdisaster: Generates error-correction data for optical disc [15].

❖ FileSalvage: A Mac OS X recovery program [16].

❖ GetDataBack: A Windows recovery program [17].

❖ Norton Utilities: A suite of utilities that has a file recovery component [18].

❖ PhotoRec: Multi-platform free and open source console program used to recover files [19].

❖ TestDisk: Can recover files as well as lost partitions [20].

❖ TotalRecovery: backup and recovery system, can work pre boot [21].

❖ TuneUp Utilities: A suite of utilities that has a file recovery component [22].

- Forensics
- The Coroner's Toolkit: A suite of utilities aimed at assisting in forensic analysis of a UNIX system after a break-in [23].
- The Sleuth Kit: Also known as TSK, The Sleuth Kit is a suite of forensic analysis tools developed by Brian Carrier for UNIX, Linux and Windows systems. TSK includes the Autopsy forensic browser [24].
- EnCase: A suite of forensic tools developed by Guidance Software that is used for imaging and forensic analysis for UNIX, Linux, and Windows systems [25].

B. Honeypots

In case of Cyber Crime, Honeypots can be described as a computer or a website which is a part of the huge network and which does not requires much authentication. But it is not so, Honeypot is isolated and being closely monitored by whoever set the trap. For example credit card fraud ring may contain fake credit card account information and other lures to attract a criminal in the ring to illegally access it and remotely, the information may be revealed by the criminal on the location who is monitoring the honeypot [26].

C. IP Address Tracking

An Internet protocol (IP) address is a number assigned to a computer or other device on a network accessing the Internet. This number can reveal specific information about the computer that is using it, such as a general location or even the name of the owner. Tracking software can be used in order to create information logs of IP addresses used by criminals in the commission of a crime. Because IP addresses can be hidden, "bounced" from computer to computer or even altered, success using this software depends on the level of skill of both the person using it and the person committing the crime [27].

D. Chat Room Monitors

Chat rooms, online gatherings of individuals interested in a particular subject who talk to each other in real time, are sometimes a target for law enforcement investigations. A popular website for children may attract paedophiles, and an officer or agent will go online and pose as a member of the chat room in order to catch the paedophile in the act of soliciting a minor. Programs are now used to monitor and record chat sessions, as well as flag any words or phrases specified by the person using the program.

Documentation Tools for Cyber Crime investigation

These tools are used for preparing documents on the spot for several purposes. These documents are prepared for issuing document copy on the spot to the organization/person, for noting down all the statements of the witness with efficiency, for presenting questionnaire to the witness and for many other purposes. These may also be used for generating spontaneous reports of the evidences and audit progress. These documentation tools are computer based basically and carried along with the auditing team. Some of the basic tools that can be referenced are DFD, ERD, Decision Tree, Decision Table, Flowcharts etc. Brief introduction of these tools are:

A. DFD

Data Flow Diagram is a graphical representation of the "flow" of data through an information system, modeling its process aspects. Often they are a preliminary step used to create an overview of any model, which can later be elaborated. DFDs can also be used for the visualization of data processing. A DFD shows what kinds of data will be input to and output from any system/model, where the data will come from and go to, and where the data will be stored. It does not show information about the timing of processes, or information about whether processes will operate in sequence or in parallel

B. ERD

An entity-relationship diagram is a graphical depiction of organizational system elements and the association among the elements. E-R diagrams can help define system boundaries. The elements that make up a system are referred to as entities. A relationship is the association that describes the interaction between entities. Basically ERD is used for visualization of flow of data contents which helps in decision making.

C. Decision Tree

A decision tree is a decision support tool that uses a tree-like graph or model of decisions and their possible consequences, including chance event outcomes, resource costs, and utility. It is one way to display an algorithm. Decision trees are commonly used in operations research, specifically in decision analysis, to help identify a strategy most likely to reach a goal. Another use of decision trees is as a descriptive means for calculating conditional probabilities. A decision tree (or tree diagram) is a support tool that uses a tree-like graph or model of decisions and their possible consequences, including chance event outcomes, resource costs, and utility.

D. Flowchart

It a type of diagram that represents an algorithm or process, showing the steps as boxes of various kinds, and their order by connecting these with arrows. This diagrammatic representation can give a step-by-step solution to a given problem. Process operations are represented in these boxes, and arrows connecting them represent flow of control. Data flows are not typically represented in a flowchart, in contrast with data flow diagrams; rather, they are implied by the sequencing of operations. Flowcharts are used in analyzing, designing, documenting or managing a process or program in various fields.

E. Data Dictionary

It is nothing but repository of data items handled in an organization or in a system. Through these data dictionaries, developers can find out what data is being used in which system and whether it has been already defined in some other system.

References

[1]. Majesty, H., Cyber Crime Strategy, S.o.S.f.t.H. Department, Editor. 2010, The Stationery Office Limited: UK. p. 42.
[2]. Grabosky, P., Requirements of prosecution services to deal with cyber crime. Crime, Law and Social Change, 2007. **47**(4): p. 201-223.
[3]. Seetharama, S., Information Management: Tools and Techniques. DRTC Workshop on Information Management Including ISO 9000 QMS, Bangalore, India, 1999.

[4]. Rogers, M.K., K. Seigfried, and K. Tidke, Self-reported computer criminal behavior: A psychological analysis. Digital Investigation, 2006. **3**(Supplement 1): p. 116-120.
[5]. Mackenzie, E. and K. Goldman, Computer abuse, information technologies and judicial affairs, in Proceedings of the 28th annual ACM SIGUCCS conference on User services: Building the future2000, ACM: Richmond, Virginia, United States. p. 170-176.
[6]. http://en.wikipedia.org/wiki/Knoppix.
[7]. http://www.grc.com/sr/spinrite.htm.
[8]. http://www.sysresccd.org/Main_Page.
[9]. http://www.trinityhome.org/.
[10]. http://support.microsoft.com/kb/314058.
[11]. http://en.wikipedia.org/wiki/Fsck.
[12]. http://en.wikipedia.org/wiki/Disk_First_Aid.
[13]. http://en.wikipedia.org/wiki/Disk_Utility.
[14]. http://www.cdroller.com/htm/article.html.
[15]. http://en.wikipedia.org/wiki/Dvdisaster.
[16]. http://www.subrosasoft.com/OSXSoftware/index.php?main_page=product_info& products_id=1.
[17]. http://www.runtime.org/.
[18]. http://us.norton.com/norton-utilities/.
[19]. http://www.cgsecurity.org/wiki/File_Formats_Recovered_By_PhotoRec.
[20]. http://en.wikipedia.org/wiki/TestDisk.
[21]. http://en.wikipedia.org/wiki/TotalRecovery.
[22]. http://www.farstone.com/software/total-recovery-tools-soft.php.
[23]. http://www.porcupine.org/forensics/tct.html.
[24]. http://www.sleuthkit.org/.
[25]. http://www.guidancesoftware.com/.
[26]. http://en.wikipedia.org/wiki/Honeypot_(computing).
[27]. A.R.Gonzales, Investigations Involving the Internet and Computer Networks. 2007: U.S. Department of Justice Office ofJustice Programs, NIJ.