Volume 4, Issue 5, May-2017, pp. 180-184 ISSN (O): 2349-7084

International Journal of Computer Engineering In Research Trends

Available online at: www.ijcert.org

Survey on current Digital forensic practices

Divith Devaiah M.M [1], Prakash B Metre [2]

[1] Student, Information Science Dept. , Acharya Doctor Sarvepalli Radhakrishnan Rd, Bengaluru, Karnataka 560107, India. [2] Assistant Professor, Information Science Dept. , Acharya Doctor Sarvepalli Radhakrishnan Rd, Bengaluru, Karnataka 560107, India.

divithd@gmail.com [1], Prakash.metre@gmail.com [2].

Abstract:- Cyber-crimes are taking over the world like a breeze. For every crimes committed around the globe, one or the other form of computer or any electronic device is used. So every crime can be linked as cyber-crime. To investigate these crimes, a cost friendly and easily available forensic device is required, which helps in collecting, analyzing and preserving data from which results can be extracted. This paper illuminates all the practices that are currently in place and also clarifies the effects of vulnerabilities.

Keywords: Cyber Crimes, Cyber Criminal, Forensic, Forensic tools, Vulnerability, Criminology, agile tool.

1. Introduction

There are around 3.7 billion people who are currently online according to a survey in 2016 and it is still growing rapidly. As PC technology is involved in everyday deeds, it has been a vital part of our lives. When the dependency surges, all our personal lives are allied with the device. When the information which are stored in the devices linked to the internet, Criminals can easily interpret such data and snip the information which are available.

Thus cyber-crimes take place and are developing rapidly in this era. The various types of cyber-crime are Phishing attacks, email hijacking, denial of service (DOS), hacking, Phreaking, pornography, Virus, Trojans, Malware, social engineering etc. Largely when crimes take place, individuals seek the help of forensics to get their problems resolved or recover the sensitive information which has been stolen. Thus requiring Forensics for the process which in turn requires sophisticated tools to get the job thru [1].

Vulnerabilities can be defined as the various loopholes that are present in a lively website. These vulnerabilities help the hackers to gain access to the servers where the hackers are able to steal the sensitive material that are present in the database. Vulnerability analysis is a procedure where certain forensic tools are used to scan and determine the various flaws that are existent in a particular website [3].

These tests are largely conducted manually or automatically. A detailed report is generated after the vulnerability analysis and the result is thoroughly understood and the security researcher conducts tests based on the type of the vulnerability which was perceived. The final objective is to find the various flaws and configure the server or the system in such a way that the certain vulnerability is eliminated and there are no loopholes left in the system [7].

2.Digital Forensic Procedures

Digital forensic is all about the numerous evidences from the computer systems that are sufficiently trustworthy to be produced in the court and which are supposed to be undoubted. The digital evidence can be found in PC's, Cell Phones, Cameras, CD's and various other communication devices such as Routers, Modems Servers etc. which has the ability to store diverse data in them.

Digital evidence can be concealed in Photos, Encrypted files, hard drives, transcripts etc. which has to be decoded to obtain fruitful information. These various evidences can relate to the various cyber-attacks and criminal activities that take place.

The procedures used in Forensics are alike and accomplished by all the investigators. The basic steps of forensic measures are listed in the figure 1 below [2].

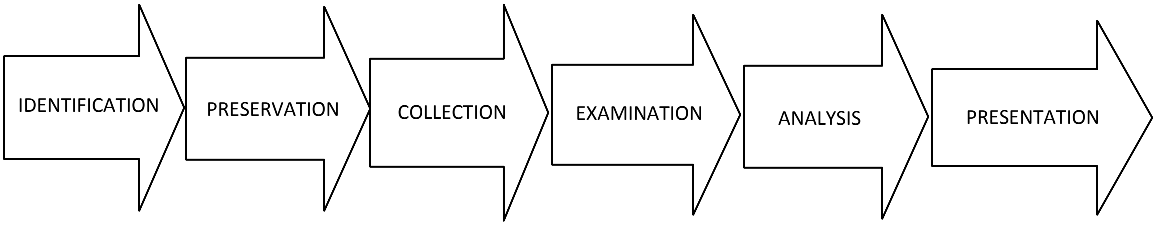

Figure 1. Forensic investigative steps

The Digital forensics process Steps are listed as Identification, Preservation, Collection, Examination, Analysis and Presentation [2, 3].

Identification: It is a step in forensic procedure where the digital evidence is collected from a particular crime scene which links to the investigation and provides leads to the particular case or which has the potential to solve the case itself.

Preservation: This Step involves preserving the collected evidence so that it stays intact until the particular issue is resolved. The preservation is usually done followed by a backup procedure so that the investigators don't lose the data or mishandle the evidence such that it is rendered useless.

Collection: Step where all the evidence which are relevant to the case or the crime are collected and sorted out which will ease out the investigators task in the solving of the case.

Examination: This involves close observation and testing the forensic evidence. Many relevant Forensic tools are used in this step by an investigator.

Analysis: Thorough examination is done in the beginning and analysis is done to find out the appropriate methods to extract the information from the obtained evidence.

Presentation: When the Analysis is finished, a conclusion is drawn over the investigation. The detailed report from the analysis is presented as the evidence by the investigators.

These processes are used in forensic analysis of cyber-crimes.

3. Tools used in forensics

The forensic tools are usually classified into various Categories:

- Disk Data Capture tools
- File analysis tools
- Registry analysis tools
- Email analysis tools
- Network forensic tools
- Mobile device forensics tools
- Database analysis tools etc.

Because of the diversity in the cyber-crimes, these are various set of tools used by the investigators based on these categories. The preference of tools are entirely dependent on the investigators choice [11].

The leading OS which is currently used in forensic is KALI. This open source operating system is available to every developer, security researcher or Forensic enthusiast around the globe who work together for the development and improvement of the operating system and the forensic toolkits. Some of the forensic tools used in the current era are [5, 9].

3.1. Digital Forensics Framework

The tool is open source has acquired GPL license. It can be utilized to access remote or local devices, Forensic of Windows or Linux OS, recovery of hidden or deleted files and various other things.

3.2. CAINE

The open source OS Computer Aided Investigative Environment (CAINE) is the Linux distro created for digital forensics. It offers and environment to combine the existing software tools as software modules.

3.3. EnCase

EnCase is another multi-purpose forensic platform which collates with many forensic tools for use in several areas of the digital forensic process. The tool is not open source and requires a paid license to be activated.

3.4. Registry Recon

It is a registry analysis tool which extracts the registry information from the evidence system and rebuilds the registry representation. It has the ability to rebuild registry from even the previous windows installations made on the system.

3.5. Volatility

It is a memory forensic tool which is mainly used in incident response and also malware analysis. This tool is able to extract information from running processes, DLL's Registry and other crucial places.

3.6. X-Ways Forensics

This is an advance platform for digital forensics examiners. It runs on all the windows versions and works very efficiently. The key features of the tool are:

- Disk imaging and cloning
- Support various file systems such as NTFS, FAT12, FAT16, FAT32, EXT2, Next3 etc.
- Recover deleted hard drive files.
- Bulk hash calculation.
- Activity logging.
- RAM analysis.
- Registry reports etc.

These are some of the forensic tools and operating systems that are used in forensic practices.

4. Digital forensic incident response

Incident response is a process where a crime scene is surveyed and entire area is swept to find out the evidence traces which leads in concluding the case. Usually these procedures are handles by professionals who has proper training and is certified to handle evidence without any mishaps.

There are various rules that need to be followed to successfully acquire the required digital evidence. If the procedure isn't followed correctly, the evidence might be rendered useless. The investigator must be well aware of the following rules and regulations [8]:

- Acquire the data without varying or damaging the genuine one.
- Verify that the recuperated evidence is the same as the originally seized data.
- Analyze the data without modifying it.

The obstacles which the investigators face during the evidence recovery are [9]:

- Identify the relevant evidence to the crime.
- Deleted data searching is waste of time.
- Find ways to read encrypted or password protected files.
- Identify tools and technique for every unique case.
- Protect acquired original data from alteration.

The obstacles usually suggest that a common method to obtain and preserve the digital evidence must be used. The most common methods in obtaining and preserving data are usually divided into several parts:

- Locating data.
- Capturing data and
- Preserving data.

5. Vulnerability analysis

The practice of identifying, Quantifying, and prioritizing the various vulnerabilities in a system is known as vulnerability assessment [3]. The tools are used only when various types of vulnerabilities are identified. Some of the vulnerability types are listed as follows [4]:

5.1. Buffer overflow.

It occurs when an application attempts to write data past the end of a buffer. It usually causes application to crash and also able to compromise data and also provide attack vector to hackers.

5.2. Un-validated inputs.

Any of the input received by the program from an untrusted sources is like a target for attack. We must check all the inputs received by our program to make sure that the data is authentic.

5.3. Race conditions.

This exists when changes to the order of two or more instance can cause change in the response. An attacker can gain access and introduce malwares to the system.

5.4. Access control problems.

Access control is the process of assigning control to various users for various access. Lot of security vulnerability exists because of the improper management of access control or fail to utilize all of them.

5.5. Cross-site Scripting (XSS).

It is a kind of security vulnerability discovered in web application where a hacker can inject client side scripts into the web pages which are utilized by various users. There are types of XSS attack:

- Persistent XSS.
- Non-Persistent attack.

5.6. Sql Injection (SQLi).

This is a technique where hackers can inject SQL commands through input of a web page in an SQL statement. The command then alters the SQL statement and compromise the security. This attack can read the data and obtain escalated privileges to the system.

5.7. URL Access restrict failure.

This vulnerability can bypass security by accessing files directly instead of routing through the link. This is one of the most common vulnerability listed on Open Web application security project (OWASP).

There are several tools which help investigators extract reports on various loopholes and security vulnerability in the system and also help them test out the system security status and evade all the existing vulnerabilities:

- Wireshark.
- Nmap
- Metasploit.
- OpenVAS.
- Aircrack.
- Nikto.
- Samurai framework.
- Safe3 Scanner.
- Websecurify.
- SQLmap etc.

6. Challenges in Digital forensics

As the pressure on digital forensics increases, the challenges also increase. There are many issues that an investigator faces during the forensic procedure such as [2, 9]:

6.1. Data InconsistencyL

Finding genuine evidence is a tough job for the investigators. The Data which are recovered in the crime scenes are inconsistent and might be misleading during the investigative process. Data usually are corrupted or destroyed after the crime and they are not trust worthy. Hence this is a big challenge in the digital forensic field.

6.2. Volume of evidence.

The amount of evidence recovered from the scene plays an important role in the investigative procedure. Less evidence which lead nowhere is practically useless.

6.3. Whole drive encryption.

When the entire drive which has been retrieved and found encrypted, it is not possible for the investigators to solve the case easily.

6.4. Technology gap

Regular update of the existing technology is a must for forensics if the investigator sticks to his old practices, it might not help him in any way. So regular training is a must for the investigators.

6.5. Technology and tools.

Since the security is breached on a regular basis by using various new technologies, it is hard to find tools which help the investigators to properly handle the evidence.

6.6. Virtualization

This area has developed very rapidly and hence recovering the data which has been manipulated is hard for the investigators to retrieve and used for investigation.

6.7. Security-awareness

The lack of awareness across the individuals contribute to around half of the cyber-crimes that are taking place in the society.

There are still many challenges that the investigators face every day. The technology is improving so rapidly that it is difficult to keep up with the current world which is entirely powered by internet.

7. Conclusion

Forensic is a must process for this digital era. Individuals around the globe are constantly trying to use the technology available for harmful purposes. There is a chance that the cyber-crimes will be increased rapidly and despite all the security measures taken, hackers will find a way to breach the system and gain unauthorized access. Current forensic practices are doing its bit but there is a lot to improve in various areas. There is a need for portable cost friendly forensic tools necessary. Awareness is a must for all individuals because at the end of the day you are your own firewall. Although few of the forensic procedures are obsolete currently, there is always a room for future enhancement in the forensic field.

REFERENCES

1. Malek Harbawi and Asaf Varol, "The Role of Digital Forensics in Combating Cybercrimes".
2. M. Al Fahdi, N.L. Clarke and S.M. Furnell, "Challenges to Digital Forensics: A survey of researchers & practitioners attitudes and opinions.
3. B.Skaggs, B. Blackburn, G. Manes, S. Shenoi, "Network Vulnerability Analysis".
4. Prashant S. Shinde and Prof. Shrikant B. Ardhapurkar, "Cyber Security Analysis using Vulnerability Assessment and penetration Testing".
5. Abirami Sivaprasad and Smita Jangale, "A Complete study on Tools and Techniques for digital Forensic Analysis".
6. Andrw Jones and Stilianos Vidalis and Nasser Abouzakhar, "Information Security and digital forensics in the world of cyber physical systems".
7. Arun V. Sathanur and David J. Haglin, "A novel centrality Measure for network-wide cyber vulnerability assessment".
8. Arni Ariani, John Lewis and Pradeep K. Ray, "The vulnerability assessment for Emergency response Plans".
9. C.Balan, Dija S, Divya S, VIdyadharan, "The need to adopt agile methodology in the development of cyber forensic tools".
10. S.Al Sharif, F.Iqbal,T.Baker and A. Marrington, "Magec:An image searching tool for detecting forged images in forensic investigation".
11. Noble Kumari and A.K Mohapatra, "An insight into digital forensics branches and tools".
12. Simson L Garfinkel and Nicole Beebe, Lishu liu, "Detecting Threatening insiders with lightweight media forensics".