Internet Forensics: Review

Gayatri Sawale
Assistant Professor,
Information Technology
Atharva College of Engineering,
India

Reena Somani
Assistant Professor,
Information Technology
Atharva College of Engineering,
India

Ashmita Shetty
Assistant Professor,
Information Technology
Atharva College of Engineering,
India

Amruta Mhatre
Assistant Professor,
Computer Engineering
Atharva College of Engineering,
India

***Abstract*— Now a day's use of internet is increasing rapidly so cyber crimes are also growing explosively. As the cyber crimes are raising so field of Internet forensic is emerged. People who do such things do not leave any forensic evidence. Such Cyber crimes are in huge area such as piracy to identity theft and beyond. Internet Forensics involves collecting and examining all evidences of digital crime which include network traffic, network devices, storage devices, mobile devices etc. This paper we discussed various attacks that happened for attacking vulnerable site, for identity theft to reduce the performance of system so legitimate user can't get access. In this paper, I have proposed a tool which is the combination of digital forensic which performs investigation and crime data mining. The proposed system is designed for finding pattern of cyber attacks, for finding motive and counts of attacks types happened during a period. Hence the proposed system enables the system administrators to reduce the system vulnerability.**

***Index Terms*— Cyber Crime, DDoS Attack, Digital forensics, Internet forensics.**

I. INTRODUCTION

The internet is riddled with spammers, con artists and identity thieves. More than a nuisance these are real crimes targeting vulnerable members of society as their victims.

A digital forensic investigation is an inquiry into the unrecognized or questionable activities in the Cyber space or digital world. Internet forensics shows you how to find these clues left behind at an Internet crime scene. Internet forensic is a practical guide targeted at programmers and system administrators. Thus, to prevent all types of attacks through websites and other platforms, and secure the Internet crime scenes, we need to be aware of the sources of these attacks and be able to use the available tools effectively.

Forensic science is a scientific field that is applied to the field of law. Forensic scientists perform the collection, preservation, and analysis of scientific evidence during the course of an investigation.

II. LITERATURE SURVEY

A. Introduction

Forensic science is the scientific process of gathering and examining information about the things happened past which is then used in a court of law

Digital forensics, a term used in computer forensics, is a branch of forensic science enclosing the recovery and investigation of material found in digital devices, often in relation to computer crime, which has elaborated to cover investigation of all devices capable of storing digital data.

Computer forensics (sometimes known as computer forensic science) is a branch of digital forensic science associating with the legal evidence found in computers and digital storage media which can deal with a broad range of information; from logs (such as internet history) through to the actual files on the drive

Network Forensics investigations deal with volatile and dynamic information. Network traffic is transmitted and then lost, so network forensics is often a pro-active investigation, which relates to monitoring and analysis of computer network traffic both local and WAN/internet, for the purposes of information gathering, legal evidence, or intrusion detection

Internet Forensics, the investigation of criminal activity that has occurred on the Internet, which deals with the analysis of the origins, contents, patterns and transmission paths of e-mail and Web pages as well as browser history, web server scripts and header messages.

Digital forensics has become rapidly crucial as an Approach to investigate cyber and computer assisted crime.

Digital forensics has become an vital tool in the identification of computer-based and computer-assisted crime.

They are ubiquitously utilized within law enforcement to investigate electronic media and increasingly within organizations as part of their incident response procedures.

Significance of Data is more vital, in this new age, so security has become a major issue in the IT industry. Cyber attacks and Digital forensic is a relatively new field that is the collection, analysis and documentation of a Cyber attacks.

The challenges on criminal oversight are classified into three categories

- Technical challenges – e.g. differing media formats, encryption, steganography, anti-forensics, live acquisition and analysis
- Legal challenges – e.g. jurisdictional issues and a lack of standardized international legislation.
- Resource challenges –e.g. volume of data, time taken to acquire and analyze forensic media

Digital forensics investigators have access to ample variety of tools, both commercial and open source, which assist in the preservation and analysis of digital evidence.

An established forensic analyst mines the vital evidence from perceptive locations to comprehend attacks and attackers intension. The typical goal of an investigation is to collect evidence using generally acceptable methods in order to make the evidence should be get accepted and admitted on the court. Efficient digital Tools and procedures are needed to effectively search for, locate, and preserve all types of electronic evidence.

Different types of cyber attacks from various sources may adversely affect computers, software, a network, an agency's operations, an industry, or the Internet itself.

Digital forensics is dealt with science of identifying, extracting, analyzing and presenting the digital evidence that has been stored in the digital devices.

In the course of the investigation, the investigator should assure that digital evidence is not modified without proper authorization.

Forensic tools and techniques are integral part of criminal investigations which is used to investigating suspect systems, gathering and preserving evidence, reconstructing events, and assessing the current state of an event.

B. Cyber Crime

An electronic crime is coined as an illegal activity that is carried out using a computer or electronic media. A cyber crime is an electronic crime that is performed using the Internet, or a crime whose “crime scene” is the Internet. Cyber crimes are not inevitably new crimes; which involve types of crimes where criminals exploit computing power and accessibility to information.

Dr. Debarati Halder and Dr. K. Jaishankar (2011) define Cybercrimes as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm and damage the reputation of the victim or cause physical or mental harm and damage to the victim directly or indirectly, using modern telecommunication networks such as Internet (Emails, notice boards, chat rooms and groups) and mobile phones (SMS/MMS)".Such crimes may threaten a nation’s security and financial health.

Sources of Cyber Crime

Cyber crimes such as hacking, network intrusion, denial of service attacks, virus distribution, hijacking (a computer or network), defacing Web sites, cyber stalking, and cyber terrorism are included in this category.

Basically the computer itself becomes not only the “target” but also “Source” of the crime. That is “unauthorized access” to the targeted system. The transmission of a program, code, information, or command, and as a result of intentionally causes damage without authorization, to a protected computer.

C. Type of Cyber Crime

Cyber-crimes are increasing rapidly and the people who do such things try to do not leave any forensic evidence. Cyber-crimes range from piracy to identity theft and beyond. Sometimes the criminals make use of the Internet which leads to tracking the users of a Web page complex and difficult.

The crimes being violated in the cyberspace like Data theft, Internet fraud, business espionage, cyber terrorism and more are on the rise.

Intellectual Property Theft/ Data Theft:

IPR crimes like act that access to patent, trade secrets, customer data, sales trends, and any confidential information. Data is a vital asset in this modern age of Cyber world. Data is a crucial raw-material, for business organizations, I.T. Companies and Call Centers. Data has also become a crucial tool and weapon for companies, to capture larger market shares. Due to the significance of Data, in this new age, its security has become a major issue in the I.T. industry.

Damage of company service networks

This can arise if someone sets a Trojan horse, conducts a denial of service attack, installs an unauthorized modem, or installs a back door to allow others to acquire access to the network or system.

Email abuse

Email abuse takes many forms, for example: unsolicited bulk email, unsolicited commercial email, mail bombs, and email harassment, email containing abusive or offensive content.

Unauthorized access

Unauthorized access is when a person is not given a permission to use or to connect or use a system entry in a manner by the system owner.

One has not been given permission from the owner to view private accounts, messages, files or resources, By hacking one can do this viewing confidential information without permission or qualifications can responsible for legal action.

Denial of Service (DoS):

A denial of service (DoS) attack is which a user or organization is loses of the services of a resource they would normally expect to have.In a distributed denial-of-service, a single target is attacked by large numbers of compromised systems (sometimes called a botnet).

TYPES OF DDOS ATTACK:

DDoS attacks can be divided into three main categories:

1. Volume based attacks: - These consist of ICMP floods, UDP floods and other spoofed packet attacks. To utilize the bandwidth of the victim's site is the main goal of the attacker. The magnitude of the attack is measured in bits per second (Bps).

2. Protocol based attacks: - These include SYN floods, fragmented packet attacks, Ping of death, Smurf attack and more.
Consume actual server resources, such as firewall is the main goal of the attacker. The magnitude of the attack is measured in Packets per second.

3. Application layer based attack:- Zero-day attack, Slowloris etc attacks are included in Application layer based attack . The main goal of the attacker is to target the Apache, Windows or open BSD vulnerabilities and more.

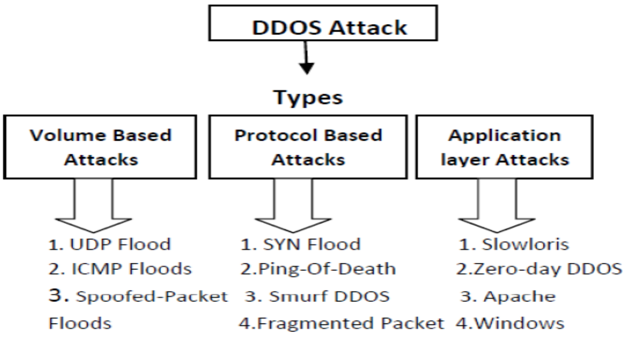

Figure 1. Types of DDoS Attack

UDP Flood

A UDP flood attack is a type of denial-of-service (DoS) attack using the User Datagram protocol (UDP), a session less or connectionless computer networking protocol.

Using UDP for denial-of-service attacks is not as straightforward as with the Transmission Control Protocol (TCP). However, a UDP flood attack can be initiated by sending a vast number of UDP packets to random ports on a remote host.

In order to determine the requested application, the victim system processes the incoming data from network. In case of absence of the requested application on the requested port, the victim system sends a "Destination unreachable" message to the sender (attacker).

In order to hide the identity of the attacker, the attacker often spoofs the source IP address of the attacking packets, attacker pose himself as a legitimate user.

UDP flood attacks may also depletes the bandwidth of network around the victim's system. Thereby, the systems around the victim are also impacted due to the UDP flooding attack.

A UDP flood attack is a type of denial-of-service (DoS) attack using the User Datagram Protocol (UDP), a session less or connectionless computer networking protocol.

Using UDP for denial-of-service attacks is not as straightforward as with the Transmission Control Protocol (TCP). However, a UDP flood attack can be initiated by sending a large number of UDP packets to random ports on remote host

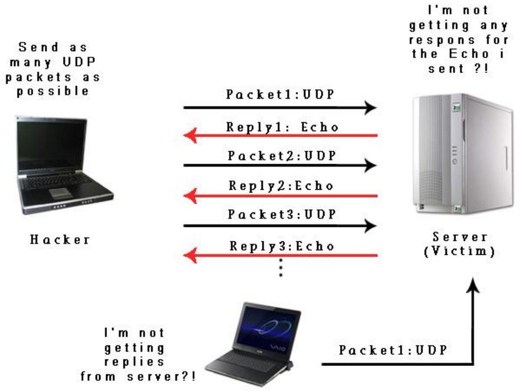
Send as many UDP packets as possible
I'm not getting any respons for the Echo i sent ?!
Packet1:UDP
Reply1: Echo
Packet2:UDP
Reply2:Echo
Packet3:UDP
Reply3:Echo
Hacker
Server (Victim)
I'm not getting replies from server?!
Packet1:UDP

Figure 2: UDP Flood Attack

SYN Flood

A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.

To explain the TCP connection establishment, we assume two hosts, host A and host B (Fig. 1). First, host A sends a SYN packet to host B to request establishing a connection.
2). Then, host B replies with a SYN/ACK packet to host A to acknowledge connection request and to request establishing a connection in reverse.
3) Finally, host A sends an ACK packet to host B to acknowledge connection request. In this way TCP connection is established

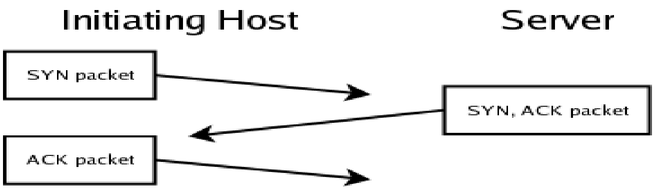

Figure 3: TCP Connection Establishment

A SYN Flood attack harms TCP establishment procedure. An overview of a SYN Flood attack is shown in Fig. 2.2

An attacker sends a large amount of SYN packets whose source addresses are spoofed, to a victim host. The victim host doesn't have means to recognize whether the source addresses of received packets are spoofed or not. Thus, the victim host responds to those spoofed addresses.
TCP protocol maintains certain status information for each data stream. The victim host could expend all of its listening queues just waiting for ACK from *source* hosts.

In other words, the victim host has to maintain and preserve half-open connection to many irrelevant hosts. The victim host is now in danger of slowing down or crashing in the worst scenario.

The slowdown of the performance of host leads to degradation of service quality which is provided by the host and if it is crashed, it cannot keep providing any services anymore. Source addresses are spoofed in SYN Flood attacks and victim replies to them automatically as we mentioned above.

This means it is possible that SYN/ACK packet arrive at irrelevant hosts abruptly. These packets are called backscatter. Capturing these packets enables us to detect SYN Flood attacks.

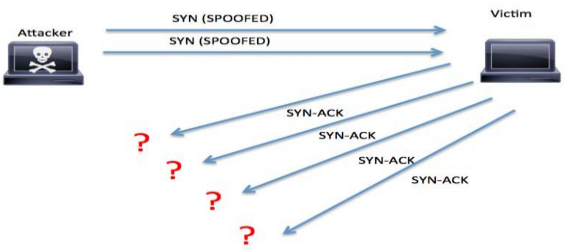

Figure 4: SYN Flood Attack

III. PREVALENCE OF INTERNET FORENSICS

Internet forensics has become an important part of safe as well as secure internet usage and an integral part of criminal investigation, where Money transfers and communication between parties can provide evidence, especially in white-collar crime.

Internet forensic consultants can use their expertise to monitor the activities in which employees engage while logged onto the company's network, this is especially important if there are employee's who have access to information the company would consider as revulsive as well as volatile or sensitive.

As the internet is growing exponentially, with more people using it every day, there are more people at risk, and more people looking to take benefit of others web insecurity. The need to protect your internet presence has necessitated the emergence and emphasized the importance of internet forensics.

IV. PROPOSED SYSTEM

We propose a generic framework for internet forensic analysis in this section. We formalize a methodology specifically for network based digital investigation.

Network forensics evolved as a response to the hacker community to discover and attribute the source of security attacks

The proposed framework is generic as it aggregates many of the phases available in the digital forensic models but builds on those phases which are specific to network forensics. The phases of proposed framework are shown in Figure 4.

1. Preparation and Authorization

The required authorizations to monitor the network traffic are obtained and a well defined security policy is in place so that privacy of individuals and the organization is not violated. It means we provide proper authentication facility to analyzer by providing log-in id and password.

2. Detection of Incident / Crime

Any unauthorized events and anomalies noticed and observed will be analyzed. The presence and nature of the attack is determined from various parameters. A quick validation is done to assess and confirm the suspected attack.

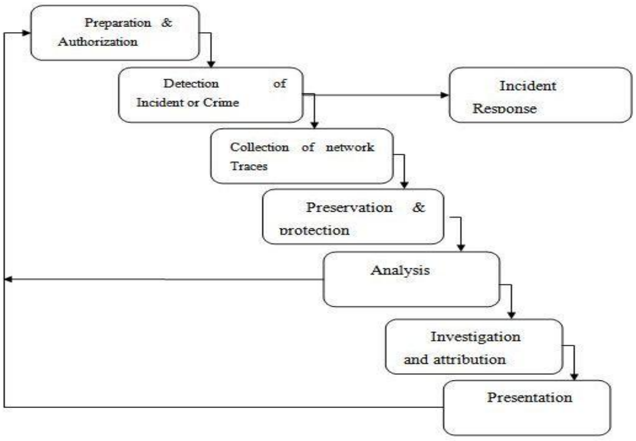
Preparation & Authorization
Detection of Incident or Crime
Incident Response
Collection of network Traces
Preservation & protection
Analysis
Investigation and attribution
Presentation

Figure 4: Phases of Prosed Framework System

3. Incident Response

The response to the crime or intrusion detected is initiated based on the information gathered to validate and assess the incident. The response initiated depends on the type of attack identified.

4. Collection of Network Traces

Data is acquired from the sensors used to collect traffic data. A well defined procedure using reliable tools, hardware and software, must be in place to gather maximum evidence causing minimum impact to the victim.

5. Protection and Preservation

The original data obtained in the form of traces and logs is stored on a back up device. Another copy of the data will be used for analysis and the original collected network traffic is preserved. This is done so that the investigation done may be proved again on the original preserved data to meet the legal requirements.

6. Analysis

The evidence collected is searched methodically to extract specific indicators of the crime. The indicators are classified or categorized and correlated to deduce important observations using the existing attack patterns. The collected data is categorized and clustered into groups so that the volume of data to be stored may be reduced to manageable chunks. It is easy to analyze large groups of organized data.

7. Investigation and Attribution

The information collected from the evidence traces is used to identify who, where, what, how when, and why of the incident. This will help in source trace back, reconstruction of the attack Scenario.

8. Presentation and Review

The observations are presented in an understandable language to the organizations management and legal personnel while providing explanation of the various standard procedures used to reach at the conclusion. The systematic documentation is also added to meet the requirements. The results are documented to influence future investigations and in improvement of security products.

V. CONCLUSION

This paper discuss about the Internet forensics and various types of digital forensics. Types of attacks are discussed in this paper which harms the legitimate Internet user. In Proposed System also explain phase which can include performing Internet Forensics.

REFERENCES

[1] “Challenges to Digital Forensics: A Survey of Researchers & Practitioners Attitudes and Opinions” , M. Al Fahdi, N.L. Clarke & S.M. Furnell 2013 IEEE

[2] ” Building Evidence Graphs for Network Forensics Analysis”, Wei Wang, Thomas E. Daniels Department of Electrical and Computer Engineering Iowa State University Ames, Iowa 50010

[3] “A Generic Framework for Network Forensics” , Emmanuel S. Pilli, R.C. Joshi, Rajdeep Niyogi , 2010 International Journal of Computer Applications (0975 – 8887)

[4] “ Digital Forensics and Cyber Crime Datamining”, K. K. Sindhu1, B. B. Meshram2 , Journal of Information Security, 2012, 3, 196-201 http://dx.doi.org/10.4236/jis.2012.33024 Published Online July 2012

[5] “ Digital Forensic Investigation Tools and Procedures,” K. K. Sindhu, Dr. B. B. Meshram, I. J. Computer Network and Information Security, 2012, 4, 39-48 Published Online May 2012 in MECS (http://www.mecs-press.org/)

[6] “Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics Yang Xiang, Member, IEEE, Ke Li, and Wanlei Zhou, Senior Member, IEEE” , IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 6, NO. 2, JUNE 2011

[7] “Guide to Computer Forensics “ , Richard Nolan,Colin O’Sullivan,Jake Branson,Cal Waits

[8] “Threshold Verification Technique for Network Intrusion Detection System ” ,Faizal M. A., Mohd Zaki M., Shahrin S., Robiah Y, Siti Rahayu S., Nazrulazhar B.

[9] “Crime and Criminal Behavior” , Henson, B., Reyns, B., & Fisher, B. (2011). Internet crime. In W. Chambliss (Ed.), Key Issues in Crime and Punishment: Crime and criminal behavior. (pp. 155-168). Thousand Oaks: SAGE Publications, Inc. doi: 10.4135/9781412994118.n12