Survey on Real Time Security Mechanisms in Network Forensics

Barenya Bikash Hazarika
Department of CS & IT
Assam Don Bosco University
Guwahati-781017
Assam(India)

Smriti Priya Medhi
Department of CS & IT
Assam Don Bosco University
Guwahati-781017
Assam(India)

ABSTRACT
Network forensics is a type of digital forensics which goal is to monitoring, correlate, examine and analysis of computer network traffic for various purposes like- information gathering, legal evidence, or intrusion detection. Now a days, various services like email, web, online transactions are used as network communication schemes. The purpose of this paper is to give an overview of different real time security mechanisms for forensic investigation of network communication schemes.

Keywords
Network forensics, IDS, SIDS, HIDS, AIDS

1. INTRODUCTION
Internet is growing rapidly day by day. With this growth, cyber-attacks are also growing day by day. Although attacks can be detected by some of the systems like IDS (Intrusion Detection System), it's very hard to find out the cyber criminals. However if the attackers are not traced and concealed, they might try to attack again. Therefore it is very important to use some real time security mechanisms which will be able to lessen the attacks to some extent in our system. [2]

Computer crimes can't be completely eliminated by using network security. So, to study and analyse them some technologies are needed. Computer forensic technology has become one of the most popular techniques these days. Computer forensics may be defined as a use of science and technology to investigate and establish facts in cyber-criminal. [1]

2. BASIC CONCEPT OF NETWORK FORENSICS
Network Forensics is the study of analysis of network traffic for discovering the information breaches or security policy violation. [4] It is proactive and mainly deals with dynamic information.

Network forensics has two uses-

1. Security: Network forensics are used to enhance security mechanisms. It may involve intrusion detection or monitoring network traffic.
2. Law enforcement: Network forensics are also used to get evidence for legal issues. [3]

Network Forensics use two type of methods to collect data-

1. Catch it as you can: Catches and stores the packets that pass through a particular network traffic point, it require a large amount of storage. [2]
2. Stop look listen method: This is a more powerful method. It uses a faster processor and saves only the certain information only by analysing the traffic. [2]

2.1 Network forensic process
Network forensics is a 2 step process-

1. Network packet capture: Firstly, it analyses the network traffic passing through the network.
2. Analysis of the captured network.- After capturing the network packets, it analyses the traffic and checks if there is some unwanted traffic passing through it and do some countermeasures if required.

2.2 Network Forensic model
Network forensic model consists of the following steps-

1. Preparation: Prepare to start the process.
2. Detection: Unauthorized anomalies are detected.
3. Collection: Collect the data traffic effectively in such a way that it gives us maximum information regarding illegal activities.
4. Preservation: Original data is preserved and copy of data is analysed. It is also known as hashed data.
5. Examination: Data collected from different places are integrated to a single data.
6. Analysis: The most important phase where the integrated data is analysed with the help of various statistical tools
7. Investigation: The main goal of this phase is to find out the path between the victim and the original point.
8. Presentation: This phase is used for presenting the information in an understandable language.
9. Incident Response: This step informs the system about illegal and unauthorized action. [6]

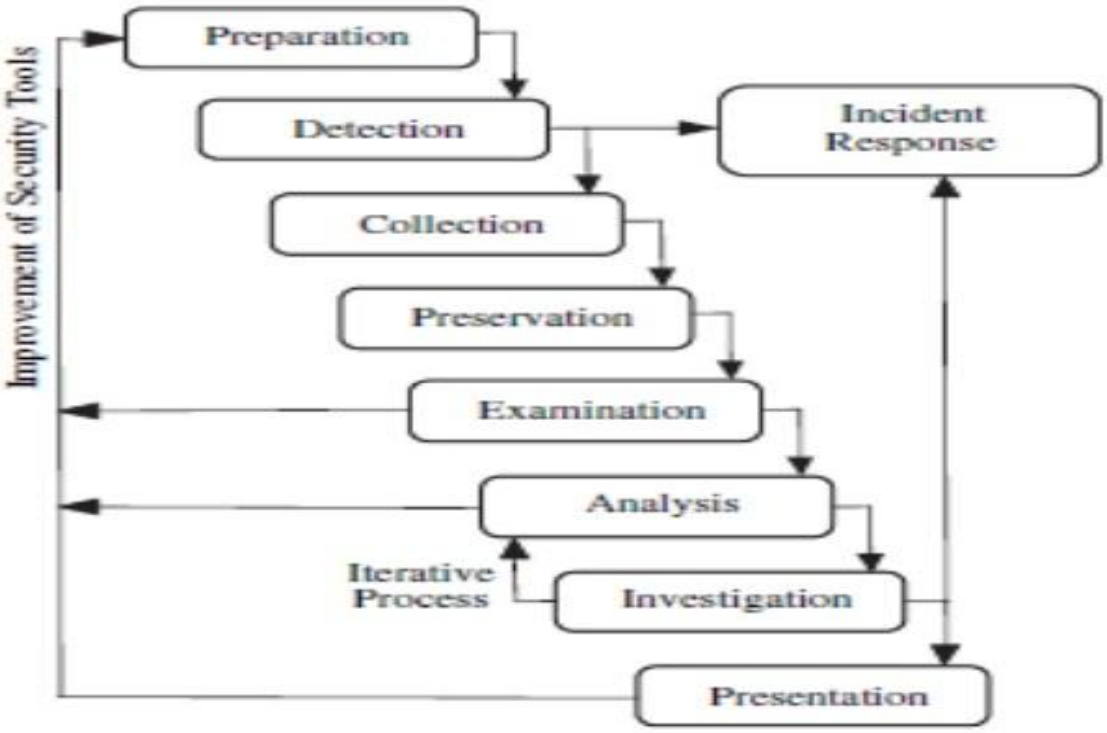

Fig.1 Process Model for Network Forensics

Fig- Network Forensic Model (source: google images)

3. SECURITY MECHANISMS

3.1 Firewalls

Firewalls are special router designed to perform inspect network traffic smartly to what should be forwarded and what traffic should be dropped or let in. It is a well-established and integral part of network security. It monitors the incoming and outgoing traffic based on some security rules. It also determines the direction in which a particular traffic may be initiated and allowed to flow through it. It works like a barrier between a secured internal network and other outside network. In an enterprise, firewalls are deployed within internal network to partition segments. A firewall can be implemented either in the IP packet layer or high IP layers. [9]

Fig- A Network Firewall(source: google images)

3.2 Honeypot forensics

Honeypot based system is to attract the attackers so that their methodology can be observed and analysed to improve defence mechanisms [3]. Any type of network device can be placed within the network of honeypots, which is known as honeynet. Honey pot is based on concept of deception. After the attacker enters into the honeypot, data is captured to identify and trace his location. It can be used to log access attempts to various ports. [6] Honeypot's services are secret, most of them are suspicious. [8].

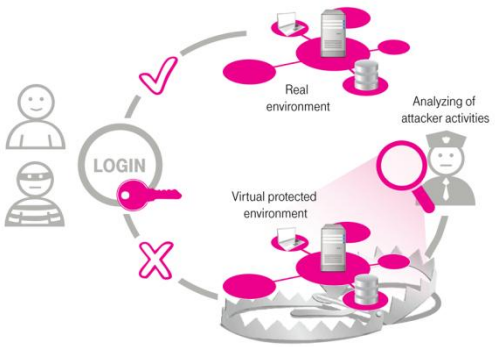

Fig-Network device honeypot (source: google images)

3.2.1 Virtual Honeypots

A virtual Honeypot is a simulated machine that can be modelled to behave as required. A system can simulate different honeypots running on different machines. Each of these virtual Honeypots can be configured with specific services that will be exploited by the attackers to gain access to a Honeypot. [7]

3.3 Email Forensics

Email is one of the most common ways of communication among peoples. It may be internal meeting requests or distribution of documents or general conversation. Emails are used for all sorts of electronic communication such as

confidentiality, authenticity, non-repudiation and also data integrity. Researchers have found that more email is generated day by day even more than phone conversations. Due to the increase in the use of email, attackers are trying to use it for malicious activities. Spam emails are the most vulnerable for attacking and are the major source of concern. Because of its vulnerability, emails can be used by hackers for secret communication. Email forensics refers to studying the source and content of electronic mail as evidence. It also studies the process of identification of the actual sender and receiver of a message, date/time it was sent and other information too. Most of the Emails may contain malicious viruses, threats and scams. It may result in the loss of data, confidential information and even identity theft. To identify the point of origin of the message, the spammers and also to identify the phishing emails that try to obtain confidential information from the receiver, some tools are used. [7] Some of them are-

3.3.1 Email Tracker Pro

Email Tracker Pro is a proprietary tool which helps identify the true source of emails to help track suspects, verify the sender of a message, trace and report spammers. The trace analysis reports the sender's IP address, estimated location, network and domain information. [1]

3.3.2 SmartWhois

SmartWhois is an open source utility software which allows us to find all the available information about an IP address, domain, hostname, including country, state, city name of the network provider, administrator and technical support contact information.

3.3.3 Comparision criteria of Email Forensic Tools

[12] et. al .refers nine criteria that may be useful in presenting the web forensic tool. They are-

1. Requirement of input file
2. Search input
3. Information provided by the tool
4. Recovery capability
5. Email file format supported
6. OS supported
7. Visualization support
8. Extended device support
9. Export format support

3.4 Web forensics

The web browsers which are popularly used now-a-days are Microsoft's Internet Explorer (IE), Mozilla Firefox, Netscape family, Safari, Google Chrome etc. Each of these browsers reveals the web browsing history of the different users who have accounts on a machine. They set up cookies during each visit. IE stores the browsing history of a user in the index.dat file and the Mozilla Firefox, Netscape family browsers save the web activity in a file named history.dat. These two files are hidden files. So, in order to view these hidden files, the browser should be set to show both hidden files and system files. These files can't be deleted easily. There is also no proof that deleting these files has speed up the browsing experience of the users [7]. There are several tools available for web forensics-

3.5 Packet Sniffers

It is a software that collects traffic flowing into and out of a computer attached to a network. Sniffers are mainly used in IDS to see if the packets are malicious or strange. There are various types of packet sniffers available-

3.5.1 Etheral

Ethereal is an open source software and widely used as a network packet analyzer. It captures packets live from the network. It displays the information in the headers of all the protocols used in the transmission of the packets captured. It filters the packets depending on user needs. Ethereal also can search for packets with some specifications. [7]

3.5.2 WinPcap(Windows Packet capture) and Aircap

WinPcap is a packet capture tool that captures the packets from the network interface of a system running the Windows Operating System. WinPcap provides support for kernel-level packet filtering and remote packet capture.

For IEEE 802.11b/g Wireless LAN interfaces, AirPcap is the packet capture tool which is popularly used. This tool is currently available only for Windows systems. AirPcap can be used to capture the control frames like CTS, RTS, management frames like Probe Requests and Responses, Authentication and data frames of the 802.11 traffic. [7]

3.6 Intrusion Detection System (IDS)

Intrusion detection systems (IDS) is a system which deals with security in a network by inspecting all the inbound and outbound traffic in the network. They monitor the network for suspicious patterns and alert the administrators when such patterns are recognized. Historically, they have been used to alert or block intruders. [5] IDS approach the goal of detecting suspicious traffic in different ways-

1. NIDS(Network Based Intrusion Detection System)-It deploys sensors at strategic locations and inspects traffic by watching for protocol violations and unusual connection patterns and malicious content. It's function is to identify abnormal behavior of a network segment. [10] [11]
2. HIDS(Host Based Intrusion Detection System)- It uses OS monitoring mechanism to find malware in the system. It monitors shell commands and system calls executed by user applications and system programs. It has the most comprehensive program information for detection and hence it is accurate. [11]
3. SIDS(Signature Based Intrusion Detection System)- It uses known misuse patterns or signatures against a stream of events for detection. It has low false alarm rates and also has precise diagnostics.
4. AIDS(Application Based Intrusion Detection System) – Is has higher accuracy and precise context but it is difficult to deploy.

3.7 Conclusion

In this paper the technical details of network forensics, its process and different security mechanisms are explored. The overview of different tools for forensic analysis is also presented.

Network forensic plays and will play a very important part in networking in future. The given brief introduction to network forensics and its real time implementation mechanisms will engender interest in the solution to the remaining problems which continue to challenge deployment of the same.

4. REFERENCES

[1] Hu Jingfang, Li busheng, "The application research on network forensics", The open automation and control system journal, 2013

[2] Amor Lazzez, "A survey about network forensics," Taif University, Vol 2 , Issue 1, January 2013

[3] Bhabesh Patel, Sanjay.M.Shah, Sameer Singh Chauhan, " Comparative analysis of Network Forensic System," IP Multimedia Communications, A Special Issue from IJCA

[4] Manesh T, Brijith Bhraguram, T M, Bhadran V K "Network Forensic Investigation of HTTPS protocol," IJMER , Sept-Oct 2013

[5] "SANS Institute InfoSec Reading Room", SANS Reading Room

[6] Gurpal Singh Chhabra, Prashant Singh " Distributed Network Forensics Framework: A Systematic Review", IJCA, June 2015

[7] Natarajan Megharathan, Sumanth Reddy Alam, Loretta A Moore "Tools and Techniques for network forensics" IJNSA ,April 2009

[8] Sven Krasser, Gregory Conti, Julian Grizzard, Jeff Gribschaw, Henry Owen, "Real Time and Forensic Data Analysis using Animated and Coordinated Visualization", IEEE ,June-2005

[9] Sherri Davidoff, Jonathan Ham "Network Forensics: trackinhg hackers through cyberspace," Prentice hall, 2012

[10] Udo Payer," Realtime Intrusion-Forensics,A First Prototype Implementation(based on a stack-based NIDS) " TERENA Networking Conferrence, 2004

[11] Pavel Laskov "Reactive Security and Intrusion Detection," Uniersity of Tubingen"

[12] Vamshee Krishna Devendran, Hossain Shahriar,Victor Clinchy, "A Comparative study of email forensics tools", Deptt of Computer Science, Kennesaw State University, Kennesaw, GA, USA, Journal of Information Security, 2015, 6, 111-117