Cyber Crime Investigation and Network Forensic System Using Honeypot

Rajni Misra
Department of Information Technology
Ludhiana College Of Engineering And Technology, Ludhiana, Punjab, India.

Dr. Renu Dhir
Department of Computer Science and Engineering
National Institute of Technology, Jalandhar, Punjab, India.

Abstract- Network Forensic is one of the most promising approaches for the network security. Under the umbrella of network security, the network forensic is regarded as the extension of the traditional security model. Apart from the general emphasis on prevention and detection of network attacks as in primitive network security model, the network forensics focuses on the collection, observation and preservation of network data so as to analyze and organize traffic data using clustering or various other data mining techniques for data verification. Here honeypots were used to lure and trick attackers using network deception, by making possible security vulnerabilities and has very good camouflage place. Also used were the various NFATs for the purpose of maximum fidelity of data collection. A prototype system is developed to collect the network logs using honeypot infrastructure and analyze all the logged traffic, which are highly malicious in nature with large volume of attacker's information. The end result of the system was to collect network data which were highly malicious in nature and were used for further investigation to get the intelligent information about the attackers as evidence for Network Forensics.

Keywords – Network Forensics, Honeypots, NFATs.

I. INTRODUCTION

With the rapid development of Internet, human activities dependent on information networks are also growing. At the same time network security is tight, and the existing security measures is mainly based on the known facts of the passive protection model. Honeypot technology is an emerging network security based on active defense technology, which by monitoring the activities of an intruder, so that we can analysis of the intruder whose skills, using the tools and motivation for the invasion, thereby enhancing network security defense capacity and also used as evidence for network forensics. At the same time, honeypots can also use the custom features to phishing attacker, slow down the attack and the transfer target, effectively make up the traditional defensive deficiencies in information security technology, makes the protection system more perfect [5].

The term Forensics to be used in science and technology to investigate and establish facts in criminal and civil courts of law. In the WWW (World Wide Web) environment, Forensics includes techniques and methodologies to collect, preserve and analyze network data on the internet for investigation purposes. It is a field of research and practice that has evolved as a result of increasing internet usage and the move of criminal activity. It is also argued that network forensics evolved as a response to the hacker community.

Digital forensics focuses on developing evidence pertaining to digital files that relate to a computer document, email, text, digital photograph, software program, or other digital record which may be at issue in a legal case. And the Network Forensics deals to collect preserve the network data evidences. It is a branch of forensic science to monitor, analyze and examine digital media or devices. The government and the corporate security firms dedicate significant resources to investigating the insider computer attacks that continue to plague organization a worldwide.

Network forensics process consists of Capturing, Collection, Preparation, Acquisition, Preservation, Examination, Analysis and Reporting [1]. Among these steps, Acquisition step is a procedure that investigators collect digital evidence and guarantee integrity of evidence at incident site. Accordingly, Acquisition step most significant step for efficient investigation.

To Develop a Network Forensic System, performs the following tasks while working with network evidences:

1. Identification: Any digital information on the network or artifacts that can be used as evidence.
2. Collection of Network data with machine learning methods for observation and then preserve that data.
3. Analyze the collected data and organize using Clustering techniques.
4. Rebuild the evidence and verify the result every time [16].

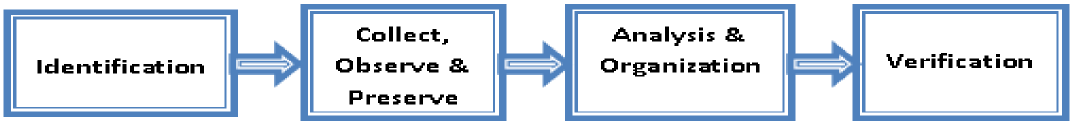


Figure 1. Processes to collect & Analyze Network data

The Collection of network evidence process to design Network Forensic System is as follow:

1. Where is the evidence? List out the systems were involved in the incident and from which evidence will be collected.
2. Establish what is likely to be relevant and admissible. When in doubt err on the side of collecting too much rather than not enough.
3. For each system, obtain the relevant order of volatility.
4. Remove external avenues for change.
5. Following the order of volatility, collect the evidence with tools
6. Record the extent of the system's clock flow.
7. Question what else may be evidence as you work through the collection steps.
8. Document each step.
9. Don't forget the people involved. Make notes of who was there and what were they doing, what they observed and how they reacted [2].

II. Working of Honeypot

The honeypot is a computer system running on the Internet which designed to lure and trick other people (such as hackers) who attempt to illegally break into others computer systems. Honeypot is mainly induced an attacker by using the network deception, makes the possible security vulnerabilities have very good camouflage place. Because honey cannot provide real value to the outside service, all of its attempt to link will be considered as suspicious. Another use of honeypots is to delay the attack on the real target, make the attacker waste time in a honeypot so that the possibility of a real network services to be detected is greatly reduced and the network detection rapidly detect the attempt of the invader. Afterward, timely repair security vulnerabilities that may exist in the system and receive the enemy's offensive skills and intentions. Honeypot tools include sensitive monitor and event log. Event log to detect an intruder to access and collect information on the activities and the same can be used as network evidences. Because any access to the honeypot system, the system is given the illusion of a successful invasion, so system administrators cannot expose the system really working conditions, timely shift, record, track intruders, to collect electronic evidence, do a better computer forensics work [5].

III. Pros & Cons Of Honeypot Technology

Honeypot technology benefits include: the fidelity of data collection, honeypots do not provide any real effect, so the data collected very little. At the same time many of the data collected is as attacks by hackers, honeypots do not depend on the detection of any complex technology, thus reducing the false negative rate and false alarm rate. The use of honeypot technology can collect new attack tools and attack methods, unlike most current intrusion detection systems use feature matching method can only detect known attacks. Honeypot technology does not require strong resources to support, low-cost equipment can be use and it doesn't require extensive capital investment. Relative other intrusion detection technologies, honeypot technology is relatively simple, enables network administrators more easily to grasp some knowledge of hacking.

Honeypot technology also has some disadvantages: the need for more time and effort. Honeypot can only attack against the surveillance and analysis, the view is more limited, unlike the intrusion detection system can listen through the bypass techniques to monitor the entire network. Honeypot technology cannot be directly protective vulnerable information systems. Honeypot deployment will bring some security risk [5].

IV. Architecting The Forensic System Using Honeypots

A. System Model Design –

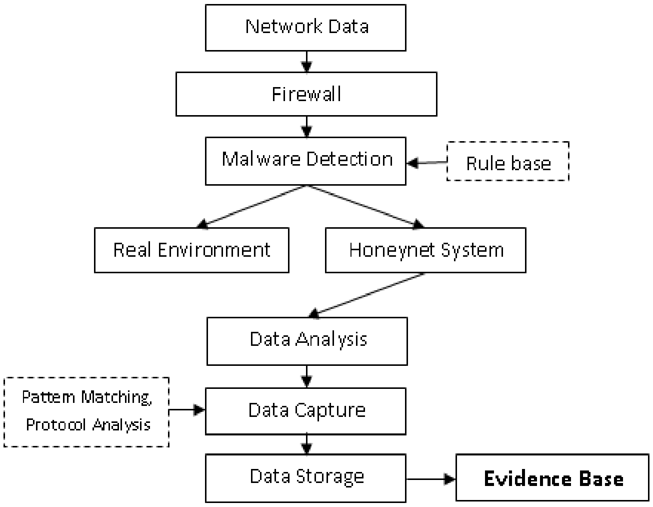


Figure 2. System Model of Network Forensic System

Computer forensics system model is the theoretical basis of forensic system. Based on the existing model into the honeypot technology, (Figure 2) gives the model of network forensics based on honeypot technology. The system has four modules, intrusion detection module, data capture module, data analysis module, data storage module.

B. System Analysis –

To address the need for protection for each machine are installed honeypot system costs too many problems, you can use technology to simulate virtual Honeypot multiple systems in order to attract more attacks or intruders. Virtual honeypot system is in a real physical machine to run some simulation software, simulation software to simulate on computer hardware, makes the simulation platform can run multiple different operating systems, such a machine becomes true multiple hosts (known as virtual machine). Virtual honeypot technology can be used to simulate the multiple systems in order to attract more attacks or intruders, software can set up a virtual honeypot system.

C. System Implementations Technology –

1) Intrusion detection module: Implementation of the network packet authentication. Intrusion detection system with rule base in comparing the rules for credible data packets allowed into the real system, suspicious packets redirected to the intrusion deception environment.

2) Data capture module: Data acquisition functions. Packet contains a record of the intruder's actions, these records will eventually help us to analyze their use of tools, strategies and attack purposes. Forensics system to collect as much as possible all available data, and ensure that these data have not been tampered with, it needs the data tansmit to Remote Security Host. We use various means to make the honeypot system to collect data integrity and security as much as possible, through a combination of several methods, it is clear replay attack the intruder. The first record is a host firewall tool. It can record all incoming and out honeypot system connections. Not only can we set the firewall to log all the connections, but also to give us warning messages. In addition, it can record some unusual port connection attempts. The second recording tool is intrusion detection system, we use Snort, configured in Linux host. It has two functions: The first role is to capture all differences in honeypot system of network data packets. In addition, it also can found some suspicious behavior and to alert you.

3) Data Analysis Module: Realize the characteristics of network data packets. Analysis of performance of the system determines the overall system performance. Therefore, it can take pattern matching and protocol analysis method to improve the analysis of system performance. Protocol analysis use the network protocol level and knowledge of relevant agreements quickly determine whether there are signatures, Thus greatly reducing the computational pattern matching to improve the accuracy of matching. Pattern matching is based on the signatures of network packet analysis technology. Its analysis speed, the advantages of small false alarm rate is unmatched by other analytical methods. Simple to use pattern matching, there are big drawbacks, we use the combination of protocol analysis and pattern matching methods to analyze network data packets.

4) Data Storage Module: Realize the data transmission and preservation. Network data packets are recognized to be safe for the invasion of the transfer of data to secure evidence of machine to prevent tampering by an intruder.

D. System Implementations –

According to the system structure, we can implement a system for Network Forensics as following steps:

1) Configuration firewall and malware detection systems.
2) In the server install VMware virtual machines to construct intrusion deception environment, then install a honeypot system in the virtual machine.
3) The establishment of legal rules on the server database using Tools for Network Forensics.
4) Configuration computer for data Analysis.
5) Configuration Forensics machine for receiving the data.

V. Tools Used For Network Forensic Process

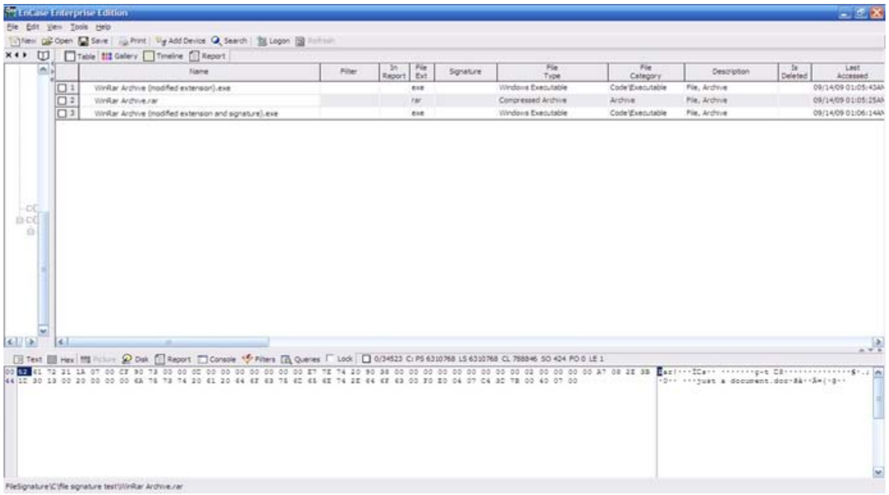
A. ENCASE –

This tool is used to analyze digital Media. It performs the following function Data acquisition, file recovery, file parsing, and hard disk format recovery. It is a network enabled incident response system which offers immediate and complete forensic analysis of volatile and static data on compromised servers and workstations anywhere on the network, without disrupting operations. It is used for the verification of the data after verifying it gives the hash value [6]. There are three components of Encase tool which are discussed below:

1. The first of these components is the Examiner software. This software is installed on a secure system where Investigations and audits are performed.
2. The second component is called SAFE, which stands for Secure Authentication for EnCase. SAFE is a server which is used to authenticate users, administer access rights, maintain logs of EnCase transactions, and provide for secure data transmission.
3. The final component is backend Servlet, an efficient component installed on network workstations and servers to establish connectivity between the Examiner, SAFE, and the networked workstations, servers, or services being investigated.

ENCASE WORKING SNAPSHOTS**:**

Below are the snapshots of the working of tool [7]:


EnCase Enterprise Edition
File Edit View Tools Help
New Open Save Print Add Device Search Logon Refresh
Table Gallery Timeline Report
Text Hex Picture Disk Report Console Filters Queries Lock

	Name	Filter	In Report	File Ext	Signature	File Type	File Category	Description	Is Deleted	Last Accessed
□ 1	WinRar Archive (modified extension).exe			exe		Windows Executable	Code\Executable	File, Archive		09/14/09 01:05:43AM
□ 2	WinRar Archive.rar			rar		Compressed Archive	Archive	File, Archive		09/14/09 01:05:25AM
□ 3	WinRar Archive (modified extension and signature).exe			exe		Windows Executable	Code\Executable	File, Archive		09/14/09 01:06:14AM

0/34523 C: PS 6310768 LS 6310768 CL 788846 SO 424 FO 0 LE 1

```
00 52 61 72 21 1A 07 00 CF 90 73 00 00 0D 00 00 00 00 00 00 00 E7 7E 74 20 90 38 00 00 00 00 00 00 00 00 00 02 00 00 00 00 A7 08 2E 3B   Rar!···ÏÇs·· ·······ç~t Ç8··············§·.;
44 1D 30 13 00 20 00 00 00 6A 75 73 74 20 61 20 64 6F 63 75 6D 65 6E 74 2E 64 6F 63 00 F0 E0 04 07 C4 3D 7B 00 40 07 00               ·0·· ···just a document.doc·ðà··Ä={·@··
```

FileSignature\C\file signature test\WinRar Archive.rar

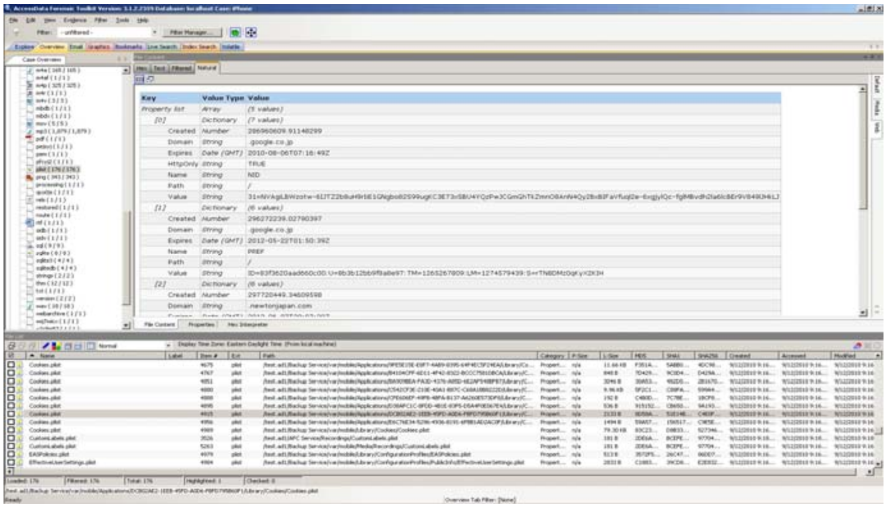
Figure 3. UI Interface of EnCase Tool

We can recover the hard disk format data with the help of Encase tool. Figure 3 shows the main screen of the encase tool. We will first select the option new and then after selecting the case option and save this new case by giving the name as your choice. Choose the drive from which you want to recover the data. After that click next and it will recover the deleted drive and the content of that hard drive successfully by this tool. By doing this we can recover the hard disk deleted data.

B. FTK Explorer –

FTK Explorer is used to locate deleted e-mails. FTK Imager is the Disk imaging program which saves an image of a hard disk in one file that may be later on reconstructed. Through this toolkit the recovery of password can be constructed. With the help of this tool from Winzip, WinRar, Gzip and compressed file data is automatically extracted. FTK processes data faster than any other computer forensics solution. It delivers true distributed processing, allowing you to divide you're processing across four workers. Furthermore, FTK is the only computer forensics solution to fully leverage multithreaded, multi-core computers. Other common forensics tools waste the potential of modern hardware solutions, while FTK will fully utilize anything you throw at it [6]. Some of the features of FTK explorer includes:

- Faster more efficient processing
- Cancel/Pause/Resume functionality
- Better real-time processing status
- CPU resource throttling
- Email notification upon processing completion.



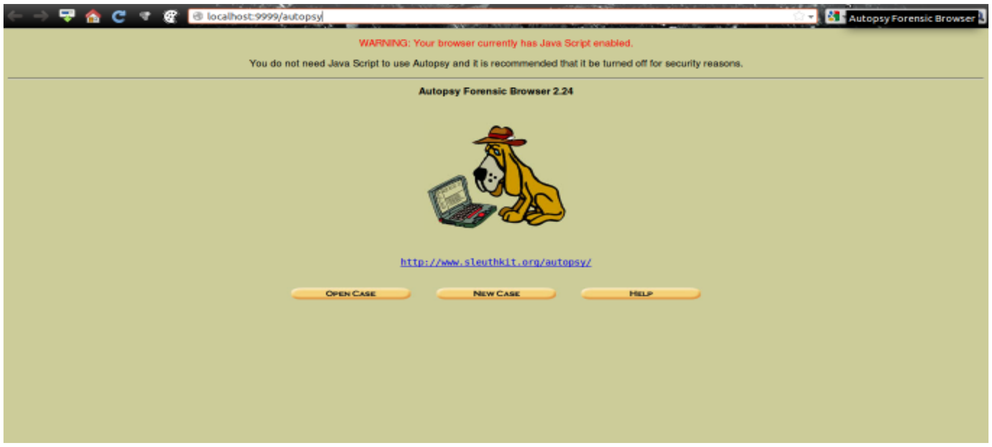
Key	Value Type	Value
Property list	Array	(5 values)
[0]	Dictionary	(7 values)
Created	Number	286960609.91148299
Domain	String	.google.co.jp
Expires	Date (GMT)	2010-08-06T07:16:49Z
HttpOnly	String	TRUE
Name	String	NID
Path	String	/
Value	String	[illegible]
[1]	Dictionary	(6 values)
Created	Number	296272239.02790397
Domain	String	.google.co.jp
Expires	Date (GMT)	2012-05-22T01:50:39Z
Name	String	PREF
Path	String	/
Value	String	[illegible]
[2]	Dictionary	(6 values)
Created	Number	297720449.34609598
Domain	String	.newtonjapan.com

Figure 4. UI Interface of FTK Explorer Tool

FTK runs in windows operating system and provides a very powerful tool set to acquire and examine electronic media.

C. SLEUTH KIT –

Sleuth kit runs on windows and Unix system. It is the file system tool allows you to examine file systems of a suspect computer in a non-intrusive fashion. Because the tools do not rely on the operating system to process the file systems, deleted and hidden content is shown. The Sleuth Kit is written in C and Perl. With these tools, you can identify where partitions are located and extract them so that they can be analyzed with file system analysis tools. The Sleuth Kit has been tested on Linux, Mac OS X and Windows [7].



localhost:9999/autopsy

WARNING: Your browser currently has Java Script enabled.

You do not need Java Script to use Autopsy and it is recommended that it be turned off for security reasons.

Autopsy Forensic Browser 2.24

http://www.sleuthkit.org/autopsy/

Figure 5. UI Interface of Sleuth Toolkit

VI.CONCLUSION

The tracking of intruder is Undeniable, so as the Honeypot technology make network security shift from passive to active defense. Compared to other security mechanisms, honeypot easy to use, flexible configuration, occupies less resources can be effective in a complex work environment, relevant data and information should be collected. With the intrusion type of diversification, the honeypot must also be a variety of interpretations; otherwise it will not be able to face the ravages of the invaders. About the tool for Network Forensics; Sleuth Kit along with Autopsy Browser has been selected as the best tool to implement for collection, analysis and to preserve the evidences for court of law. Further for the research analysis, the paper introduces the aforementioned concepts in the cyber-crime investigations domain and the suitability of the underlying tools is studied. Furthermore, a variety of network forensics tools include digital evidence bag, automated logging – network tools in particular – which could be interfaced with the Network Forensic System. By this, a more specialized system equipped with the appropriate semantics would allow further exploration of the efficiency and effectiveness of the tool. By comparing the features of these given tools in this paper, we will formulate to further design and implementation framework of network forensics system for these tools with efficient results to collect the digital evidence.

REFERENCES

[1] Kenneally, E.K., “The Internet is the Computer: the role of forensics in bridging the digital and physical divide”, Digital Investigation, Vol. 2, Issue 1, 2005, pp. 41-44.

[2] Chung-Huang Yang, Pei-Hua Yen “Fast Deployment of Computer Forensics with USBs**”,** 2010 International Conference on Broadband, Wireless Computing, Communication and Applications.

[3] Hanan Hibshi Carnegie ,Timothy Vidas Carnegie, Lorrie Cranor Carnegie Mellon University Pittsburgh, PA, USA “Usability of forensics tools: user study” 2011 Sixth International Conference on IT Security Incident Management and IT Forensics.

[4] Syed Naqvi, Gautier Dallons, Christophe “Applying Digital Forensics in the Future Internet Enterprise Systems – European SMEs’ Perspective”(CETIC) Charleroi, Belgium 2010 Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering.

[5] Zi Chen Li , Xiao Jia Li , and Lei Gong, “Computer Forensics System Based On Honeypot”, Proceedings of the Third International Symposium on Computer Science and Computational Technology(ISCSCT ’10), August 2010, pp. 336-337.

[6] Mario Hildebrandt, Stefan Kiltz and Jana Dittmann” A Common Scheme for Evaluation of Forensic Software” 2011 Sixth International Conference on IT Security Incident Management and IT Forensics.

[7] Guidance Software, EnCase. http://www.guidancesoftware.com

[8] Ashley Brinson*, Abigail Robinson, Marcus Rogers “A cyber forensics ontology: Creating a new approach to studying cyber forensics” d igital investigation 3 S (2 0 0 6) S 3 7 – S 4 3.

[9] Frank Y.W. Law, K.P. Chow, Michael Y.K. Kwan, Pierre K.Y. Lai “Consistency Issue on Live Systems Forensics”.

[10] Yong-Dal Shin* ”New Digital Forensics Investigation Procedure Model” Fourth International Conference on Computing and Advanced Information Management.

[11] Seokhee Lee, Hyunsang Kim, Sangjin Lee, “Digital evidence collection process in integrity and memory information gathering”.

[12] Dan Manson, Anna Carlin, Steve Ramos, Alain Gyger, Matthew Kaufman, Jeremy Treichelt “Is the Open Way a Better Way?Digital Forensics using Open Source Tools” Proceedings of the 40th Hawaii International Conference on System Sciences – 2007”.

[13] Marcus K. Rogers, Kate Seigfried” The future of computer forensics: a needs analysis survey” Received 21 November 2003; accepted 6 January 2004.

[14] Maria Karyda and Lilian Mitrou,” Internet Forensics: Legal and Technical Issues” Second International Workshop on Digital Forensics and Incident Analysis (WDFIA 2007).

[15] Simson L. Garfinkel,” Automating Disk Forensic Processing with SleuthKit, XML and Python” 2009 Fourth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering.