International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 4 Issue 8 August 2017

Implementation for Securing Banking Information through Network Forensics using Honeypot

Juhi Khan[1], Rajesh Kumar Chakrawarti[2]
Computer Science and Engineering, RGPV, Bhopal, Indore, 452001, India[1, 2]
erjuhikhan93@gmail.com[1], rajesh_kr_chakra@yahoo.com[2]

Abstract: *A Honey pot is an exciting new technology with enormous potential for the security community. It is resource which is intended to be attacked and compromised to gain more information about the attacker and his attack techniques. The most of the attacks by a hacker would like to attack on the database concerning the username, the password and their respective account numbers. After acquisition of the same the hackers would very conveniently trespass the security walls of authentication and authorization and thereby making the transaction official. Honey Pots are spurious computer systems, structure as a "decoy", that are used to assemble data on intruders. A Honey Pot, loaded with spurious information, views to the hacker to be a legitimate machine. While it arises defenseless to attack, it actually anticipates access to esteemed data, administrative controls and other computers. As long as the hacker is not scared away, system administrators can now collect data on the identity, access, and compromise methods used by the intruder. Honey Pots are set up to monitor the intruder without risk to production systems or data.*

Keywords: *Honey net, Network Forensics, Malware, Intruders, Hackers, Cyber Crime.*

1. INTRODUCTION

A honey pot is basically a software for information accumulate and intruder detection. A honey pot is an information system material whose value lies in the unauthorized or illicit use of that material. More generally a honey pot is a trap set to divert or discover attempts at unlawful use of information systems. This chapter introduces the basic need and domain study. The quantity of individuals interfacing with the Internet is expanding quickly. The usability and the network the Internet gives are very helpful yet the dangers included what's more, malignant interruptions are likewise expanding step by step. Misuse of PC systems is getting more normal. It is totally basic for business association and in addition people to shield their information from genuine dangers that would plan to take their data. There are numerous security arrangements accessible in the market. Some of them resemble Firewall, Intrusion Detection System (IDS), and Honey pot which are clarified beneath. The conventional framework security approach is marginally centered on barrier however more consideration has been attracted to forceful types of barrier against potential assailants and interlopers. The propelled fake based innovation called Honey pot is a comparative type of security against interruption. [1]

In both of these compositions were the beginnings of what got to be honey pots. Spear Spitzner, key individual from a examine gather in the United States called Project Honeynet, characterizes the term honeypot as takes after: "A honeypot is a asset whose esteem is in being assaulted or bargained. This implies, a honeypot is required to get examined, assaulted and possibly misused. Honeypots don't alter anything. They give us extra, important data." A honeypot is an asset, which puts on a show to be a genuine target. The principle objectives are the diversion of an assailant what's more, the pickup of data around an assault and the assailant. Honeypots don't help straightforwardly in expanding a PC networks security. It is characterized as a PC framework on the Internet that is explicitly set up to pull in and "trap" individuals who endeavor to enter different person‟s PC frameworks. Honeypot is a trap; an electronic draw. It is a PC or system assets that seem, by all accounts, to

be a part of the system yet have been conveyed as sitting duck to tempt programmers .We can characterize honeypot as a "data framework asset whose esteem lies in unapproved or illegal utilization of that asset." Most honeypots are introduced with firewalls. Honeypots and firewalls work backward heading to each different as the honeypots permit all activity to come in however hinder all cordial activity. Most honeypots are introduced inside system firewalls also, is a method for checking and following programmers. Honeypots are a one of a kind apparatus to find out about the strategies of programmers**.**[2]

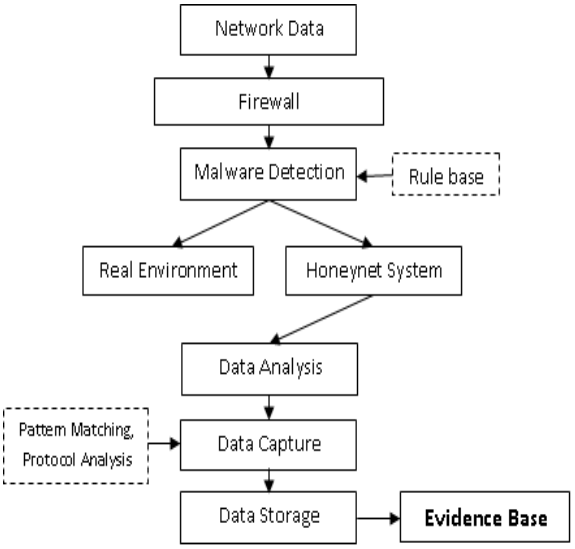


Figure: 1 Model based execution

2. LITERATURE SURVEY

Intrusion network forensics is a specific area of network forensics, applied to network intrusion activities. Network forensic science, which relates to the investigation of situations where there is digital or electronic evidence of a crime. "Intrusion forensics relates to the investigation of attacks or abnormal behavior directed against computers per Intrusion detection system uses standard computer logs and computer audit trails, gathered by host computers, or information gathering is done in networking devices such as routers and switches, for the detection and identification of intrusion process into a computer network system. Successfully reorganization of intrusion is based anomalous behavior patterns. Network forensics therefore, covers the complete activities than doe's intrusion detection task.[3]

The number of papers examining particular points concerning honeypots and how honeypots can be made and conveyed . There are number of procedures has been utilized for arrange security. The IDS can be characterized as an instrument or programming application that screens the exercises of the PC framework and additionally organize because of the potential event of malignant exercises or breaks of security approach. [4]The IDS produces reports for the control station. It is principally centered on recognizing and recording data about any occasions and also reporting comparative endeavors. The Simulating Networks with Honeyd is proposed in, in this paper Honeyd mimics virtual has on a system, furthermore, is effectively utilized as a part of Honeynet research today. The Official Nmap Project Guide to Network Discovery and Security Scanning is proposed in, which says The Nmap Security Scanner is a free and open source utility utilized by a large number of individuals for system disclosure, organization, stock, and security reviewing. Firewall gives the sifting and produces logs to encourage examine any vindictive action or any infringement strategy of get to control list, firewall rules. There are a few papers have been investigated on the honeypot, to secure information over cloud in paper. There is additionally paper on honeypot utilizing counterfeit consciousness. A few papers talks about the idea of half and half honeypot .Some paper talks about honeypot design in. There is one study has been finished by ready rationale. [5].In mid 2012, Alert Logic pushed the first in a game plan of reports on cloud security, with the target of making the IT industry‟s first assessment of security in the cloud for associations considering the use of disseminated processing stages [6]. The Official Nmap Project Guide to Network Discovery and Security Scanning is proposed in, which says The Nmap Security Scanner is a free and open source utility used by a colossal number of people for framework divulgence, association, stock, and security assessing. Nmap uses unrefined IP allocates a piece of novel ways to deal with make sense of what hosts are open on a framework, what organizations (application name and shape) those hosts are advancing, what working structures they are running, what sort of bundle channels or firewalls are being utilized, and that is just the tip of the ice sheet. [7] Have based Intrusion Detection System proposed in, it presents interference area structure which enlightens system manager about potential interference event in a structure. The arranged outline uses real technique for data evaluation that licenses distinguishing proof in light of the learning of customer activity deviation in the PC structure from scholarly profile addressing standard customer lead. Cybercrime is an unapproved arranging which is done in a PC framework, for example, phishing and

infections. Culprits began to taint PC framework with PC infections, which prompted to breakdowns on individual data and business data on PCs. PC infections are types of code or malware program that can duplicate themselves and harm or defer information and framework. At the point when PC infections are utilized on an extensive scale like with bank, government, doctor's facility organizes, these activities is classified as digital fear based oppression. PC programmers additionally take part in phishing, spam resembles requesting account no., Mastercard details [8, 9].

3. COMPARATIVE STUDY ON HONEY POT

Just inside an appropriately arranged system, one can accept that each bundle sent to the Honeypot, is suspect for an assault. In the event that misconfigured bundles arrive, the measure of false alarms will rise and the estimation of the Honeypot drops. There are two classes of honeypots – generation honeypots and research honeypots. A generation honeypot is used to moderate hazard in an association while the second classification, research, is intended to assemble as much data as conceivable. These honeypots don't increase the value of an association, yet they can comprehend the black hat group and their assaults and in addition to assemble some better resistances against security dangers. An appropriately built honeypot is put on a system, which nearly screens the activity to and from the honeypot. This information can be utilized for a assortment of purposes. In the first place, honeypots don't take care of a particular issue. They are a very adaptable device that has numerous applications to security. They can be utilized everything from backing off or halting robotized assaults, catching new endeavors to gathering insight on developing dangers or early cautioning also, forecast. Second, honeypots come in a wide range of shapes and sizes. They can be everything from a Windows program that copies normal administrations, for example, the Windows honeypot KFSensor3, to whole systems of genuine PCs to be assaulted, for example, Honeynet. Truth be told, honeypots don‟t even must be a PC, rather they can be a charge card number, Excel spread sheet, or login and secret word (usually called honeytokens) Honeypots are arranged in view of its level of communications. The word interaction here means the level of interchanges that are being took into account the aggressor to abuse the honeypot [10].

- **Low level cooperation:-**On the premise of cooperation low connection honeypots doesn‟t give Operating framework access to the gatecrasher .It gives just administrations, for example, ftp, http and so forth. These low collaboration honeypots assumes the part of inactive IDS where the system activity is not altered. A few cases of low association honeypots are honeyd, phantom, BOF.
- **Medium level connection:** Like low connection honeypots these additionally don't give OS access to aggressor yet opportunities to be examined are more than low connection honeypots .Some cases of medium connection honeypots are Nepenthes.
- **High level connection:** These are the most advanced honeypots .These are hard to plan and execution .These honeypots are exceptionally tedious to create and have most elevated dangers included with this as they include real OS with them .In high Interaction Honeypots nothing is recreated or limited. Some case of High collaboration honeypots are Sebek, Argos. All in all every activity from and to a honeypot is unapproved action.

Every one of the information that is gathered by a honeypot is in this manner intrigued information. Information gathred by the honeypot is of high esteem, and can prompt to better comprehension and learning which thus can help to increment general system security. One can likewise contend that a honeypot can be utilized for counteractive action since it can distinguish assailants from assaulting different frameworks by involving them sufficiently long and tie their assets.The table 1 appears some case of honeypot in view of their connections and reason.[11].

4. RELATED WORK

Related Work/Papers are Summarized Below

- **“Design Considerations for a Honeypot for SQL Injection Attacks”, Thomas M.Chen and John Buford, 5thWorshop on Security in Communications Networks, October 2009**. (In this Paper the Honeypot was created to **Implementation of Honeypot as an Intrusion Detection System for Wireless Network 461**emulate the appearance of common defence against SQL injection and they proposed considerations to deploy an experimental honeypot with honeyd).
- **“High Interaction Honeypot System For SQL Injection Analysis”, Wei Huang, Jiao Ma and Kun Chai, 2011 International Conference of Information Technology.** (In this Paper they proposed a high-interaction webhoneypot system for SQL injection analysis. By (i) modifying PHP extension for MySQL to intercept data-baserequests and (ii)adopting exception based and signature based detection techniques).

- **"Securing WMN using Hybrid Honeypot System", Paramjeet Rawat, Sakshi Goel, Megha Agarwal and Ruby Singh, International Journal of Distributed and Parallel Systems (IJDPS), May 2012**. (In this Paper, a Honeynet is proposed that is able to trap the hacker by analyzing their hacking techniques and thereby sending the logs information to a centralized repository to analyze those logs so as to better understand the technique used for attacking).
- **"Hybrid Honeypot System for Network Security", Kyi Lin Lin Kyaw, Department of Engineering Physics,Mandalay**. (In this Paper, they described the importance of low-interaction honeypot and high-interaction honeypot and compare the features between them. And then they proposed hybrid honeypot architecture that combines low and high interaction honeypot to mitigate the drawback).

5. IMPLEMENTATION

This paper describes the principal and dominant characteristics and attribute of honeypot by attracting the intruder/hacker and rescue the network in future.The System work as HoneyPot or the server which consist of fake websites and applications that attract the attacker/hacker. The websites have no connection with the real world, they were only meant for the attackers. If the user acts according to the Honeypot then the particular user will be blacklisted. The system belongs to research honeypots and is initially deployed on real windows platform. It imitates or copy unprotected websites, inviting hacker to attack by providing supreme information and exposing vulnerabilities.

Case Study: 1 - Fake Bank Website Attracting the Attackers

A bank login page will be shown to the attacker; he uses hit and trail method and guesses ID and password. The Honeypot will provide forgery information about some user to show him that his track or the guess was correct and now he can do the changes or transfer money from that account. Side by side the Honeypot was monitoring its unauthorized activities and blacklist the user. When the user enters the correct login and password the he would be directed to his/her account.

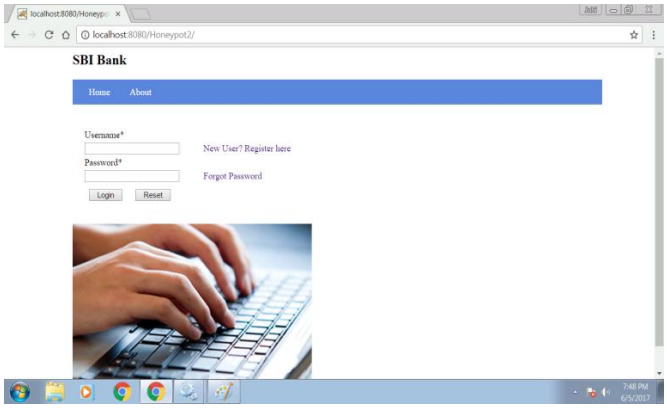


Figure 2: Login Page

The valid user would get the real page of his account and to check whether it is the real page, one can see the URL of the page where the URL contains the ValidLogin.aspx page which is directly from the Server.

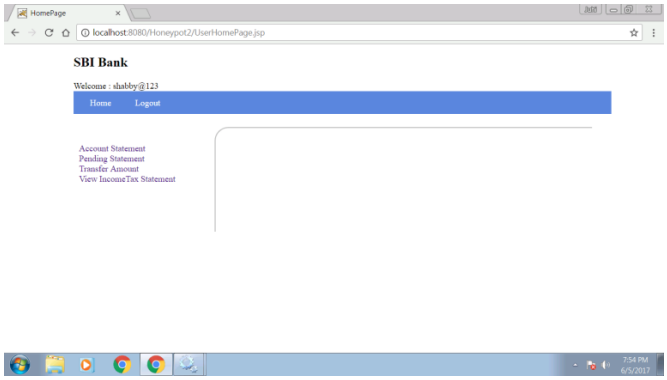


Figure 3: Valid User Page

When the attacker try to guess the password and uses hit and trail method for more than 3 times then he would be directed to the page which is exactly the same as the original valid page but it could be seen that the URL was not same as of the Valid Login Page. The URL of this page contains hacker.aspx instead of ValidLogin.aspx.

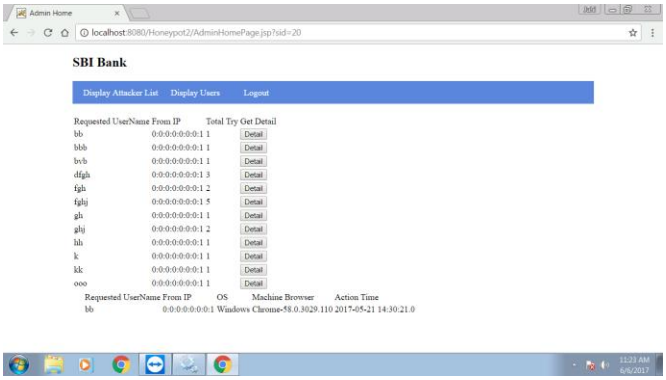


Figure 4: Hacker detail Page

Now the attacker can perform any action like Deposit as it was performed below and successful transaction would be shown but side by side the information regarding the attacker would be send to the server page of Bank and it also gives number of attempts, browser, IP address and various details about intruders.

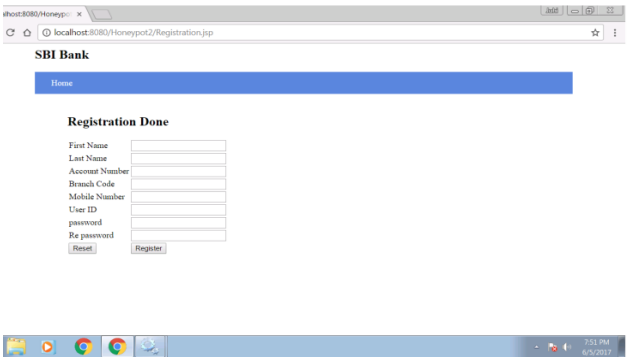


Figure 5: Registration Page

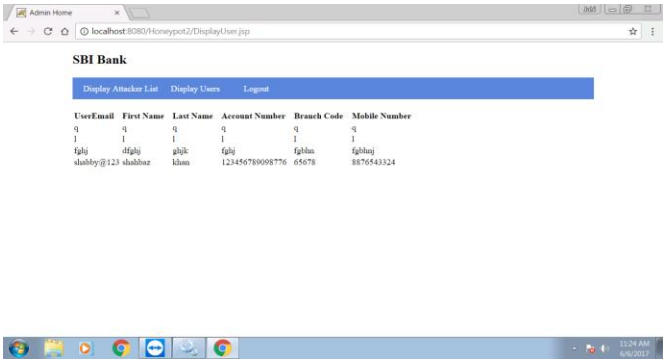


Figure 6: Valid user Page

Above shown contains the information of the valid user to the server of the Bank and various details of authorized user.

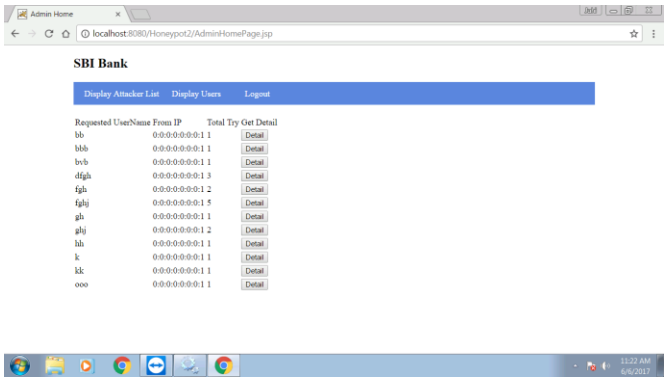
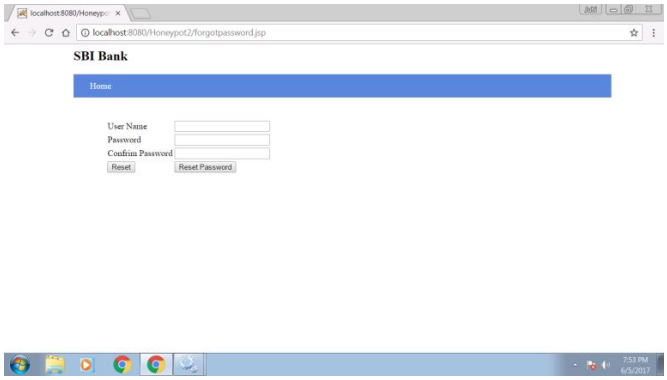


Figure 7: Server Admin Page of the Bank

Case Study: 2 - Providing Greed to the Attacker



In this a normal forgot password Page has been created with an attached message that if anybody want to know the password of others then click on the button. And after that some information is gathered from the attacker to show him that he was using a genuine site. In this way if the attacker comes in trap, a normal page with a statement "to reset the password", when the user click on the button would be directed to a page to enter the ID. If the user enters the valid Login and ID would be directed to the welcome as was not a hacker and can continue in his account.

6. PROS & CONS OF HONEYPOT TECHNOLOGY

The honeypot is a PC framework running on the Internet which intended to bait and trap other individuals, (for example, programmers) who endeavor to illicitly break into others PC frameworks. Honeypot is principally initiated an aggressor by utilizing the system misdirection, makes the conceivable security vulnerabilities have great disguise put. Since nectar can't give genuine esteem to the outside administration, the greater part of its endeavor to connection will be considered as suspicious. Another utilization of honeypots is to defer the assault on the genuine target, make the assailant squander time in a honeypot so that the likelihood of a genuine system administrations to be identified is extraordinarily lessened and the system location quickly identify the endeavor of the trespasser. A while later, convenient repair security vulnerabilities that may exist in the framework and get the foe's hostile abilities and goals. Honeypot instruments incorporate touchy screen and occasion log. Occasion log to recognize an interloper to get to and gather data on the exercises and the same can be utilized as system proofs. Since any entrance to the honeypot framework, the framework is given the hallucination of an effective intrusion, so framework executives can't uncover the framework truly working conditions, convenient move, record, track gatecrashers, to gather electronic proof, do a superior PC crime scene investigation work. Honeypot innovation benefits include: the devotion of information gathering, honeypots don't give any genuine impact, so the information gathered practically nothing. In the meantime a large number of the information gathered is as assaults by programmers, honeypots don't rely on upon the location of any unpredictable innovation, accordingly diminishing the false negative rate and false alert rate. The utilization of honeypot innovation can gather new assault devices and assault strategies, dissimilar to most current interruption recognition frameworks utilize highlight coordinating technique can just distinguish known assaults. Honeypot innovation does not require solid assets to support, minimal effort hardware can be utilize and it doesn't require broad capital speculation. Relative other interruption location advances, honeypot innovation is moderately straightforward, empowers organize overseers all the more effortlessly to handle some information of hacking. Honeypot innovation additionally has a few inconveniences: the requirement for additional time and exertion. Honeypot can just assault against the observation and examination, the view is more constrained, dissimilar to the interruption discovery framework can tune in through the sidestep methods to screen the whole system. Honeypot innovation can't be straightforwardly defensive helpless data frameworks. Honeypot organization will bring some security chance.

7. CONCLUSION

In this review paper author analyzed various tools, methods which is used under network forensic. Network forensic plays vital roles in cybercrime, various tools are used to detect various malicious programs, intruder detection system are helpful in the detection of intruders which is present inside the computer system through different processes. Honeypots based model is helpful to gather the assailant follows as anything going ahead honeypot is malignant in nature.The assault information gathered on honeynet are broke down by NIDS and prepared by the SnortAlog apparatus. The classification of these assaults has finished concerning assault sort, port and so forth with factual graphical dissemination. Contrasted and other security component found that honeypots are anything but difficult to utilize, compelling in complex environment, gathering information and data important of a decent esteem which can be later investigated forensically.In this project author use various method in combinational method to overcome the drawback of previous project and using tools and technique for detecting and collecting information of unauthorized user.

8. ACKNOWLEDGMENT

This exploration work is self financed however prescribed from the organization in order to enhance the security breaks with current procedures. In this way, the creators thank the mysterious analysts for their profitable remarks, which reinforced the paper. The creators additionally wish to recognize organization for their support and inspiration amid this examination. They additionally get a kick out of the chance to express appreciation to my guide for talk with respect to the situational mindfulness framework and for creating the approach adjusted for this paper.

REFERENCES

[1] A. Almulhem, “Network forensics: Notions and challenges,” presented at the IEEE International Symposium on, Signal Processing and Information Technology, UAE, Ajman, Dec 14-17, 2014.
[2] D. Akkaya and F. Thalgott, Honeypots in Network Security, Bachelor Project, Linnaeuos University, Sweden, 2015

[3] F. Raynal, D. Kaminsky, P. Biondi, and Y. Berthier, "Honeypot forensics, Part I: Analyzing the network," IEEE Security & Privacy, vol. 2, no. 4, pp. 72–78, July 2004.
[4] F. Raynal, D. Kaminsky, P. Biondi, and Y. Berthier, "Honeypot forensics, Part II: Analyzing the network," IEEE Security & Privacy, vol. 2, no. 5, pp. 77–80, July 2004.
[5] S.Davidoff and J. Ham. Network Forensics Tracking Hackers through Cyberspace, USA: Pearson Education, 2012.
[6] K. Scarfone and P. Mell. "Guide to intrusion detection and prevention systems (IDPS)," National Institute of Standards and Technology, Gaithersburg, NIST Special Publication, 2007, pp. 800-94.
[7] N. Provosand and T. Holz, Virtual Honeypots: From Botnet Tracking to Intrusion Detection, 1st ed. Boston, and USA: Addison Wesley Professional, 2007.
[8] T. Grudziecki et al., "Proactive detection of security incidents," Document Report, ENISA, 2012.
[9] A. Nyre, "Increasing survivability by dynamic deployment of honeypots," M.S. thesis, Dept. of Telematics, Univ. of Science and Technology, Norwegian, 2005.
[10] H. Artail, H. Safab, M. Sraj, I. Kuwatly, and Z. Al-Masri, "A hybrid honeypot framework for improving intrusion detection systems in protecting organizational networks," Computer Security, vol. 25, no. 4, pp. 274–288, 2006.
[11] N. Meghanathan, S. Allam, and L. Moore, "Tools and techniques for network forensics," International Journal of Network Security & Its Applications, vol.1, no.1, pp 14-25, April 2009.