International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Volume 1, Issue 5 (Nov-Dec 2013), PP. 07-12

HONEYPOTS IN NETWORK SECURITY

Abhishek Sharma
Research Scholar
Department of Computer Science and Engineering
Lovely Professional University (Punjab) - India

Abstract— **Computer Network and Internet is growing every day. Computer networks allow communicating faster than any other facilities. These networks allow the user to access local and remote databases. It is impossible to protect every system on the network. In industries, the network and its security are important issues, as a breach in the system can cause major problems. Intrusion detection system (IDS) is used for monitoring the processes on a system or a network for examining the threats and alerts the administrator about attack. And IDS provide a solution only for the large scale industries, but there is no solution for the small scale industries so model is proposed for honeypot to solve the problem of small scale industries which is the hybrid structure of Snort, Nmap, Xprobe2, and P0f [2]. This model captures the activities of attackers and maintains a log for all these activities. Virtualization is performed with the help of virtual machine. The focus of this report is primarily on preventing the attacks from external and internal attackers and maintaining the log file using honeypot with virtual machine [6].**

Keywords— Intrusion detection system, honeypots, attacker, security.

I. INTRODUCTION

Scale of Internet technology is very large and it is still growing every day. The security of network is required for improvement of the industries which are dependent on the internet to enhance the business and providing services on the network. So security of network is primary concern of the industries for securing the critical information. Big sums of attacks are noticed in recent years on these kinds of industries. Intrusion detection system (IDS) is used for monitoring the processes on a system or a network for examining the threats and alert the administrator. IDS and firewalls are used for protecting the system and network from attacks, but after so many efforts for security still the network is not fully secured so different types of solutions are proposed by the experts.

The small scale industries using LAN have to keep high their own security level as the database, server and clients are all handled by themselves. Since threat from internal network is Always the big challenge for the administrators, so a solution is required for small scale network to secure their internal network. This report provides the solution for the same using honeypot.

II. LITERATURE REVIEW

Honeypot is a non-production system, used for exploiting the attacker and notice the attacking techniques and actions. The objective of honeypots is not only to notice but to tackle the risk and remove it. There are various definitions of honeypots are available as few people take it as a system to confuse the attackers and inspect their activities where as other take it as a technology for detecting attacks or real systems formed for getting attacked.

In network security, honeypots are used to detect the attackers and learn from their attacks and then modify and develop the system accordingly for security. The loop holes of the network security can be covered with the help of information provided by honeypots.

Honeypot can be figured as a computer system connected with a network for inspecting the vulnerabilities of a computer or a complete network. The loopholes can be examined collectively or individually of any system, as it is an exclusive tool to study about the attackers and their strategies on the network. [3]

Honeypots are normally virtual machines which acts like a real system. Honeypots are classified into following categories on their use:

Research honeypots:
These are the honeypots which are manipulated and are used to acquire information and knowledge of the hacker society. The knowledge gained by the experts are used for the early warnings, judgment of attacks, enhance the intrusion detection systems and designing better tools for security.

Production honeypots:
These are the honeypots derived by the industries as a part of network security backbone. These honeypots works as early warning systems. The objectives of these honeypots are to remove the threats in industries. It provides the information to the administrator before the actual attack. [1] [5]

Honeypots can also be classified on the basis of level of involvement or interaction as:

Low level interaction:
Honeypots that provide only some fake services, these acts as an emulator of the operating system and services. These honeypots are simple to design but also simply detectable. Attacker can just use a simple command to identify it that a low involvement honeypot does not support. An example of this type of honeypot is *Honeyd.*

High level interaction:
High level interaction honeypots provides the real like operating systems and some real services with some real uncertainties. These allow the capturing of information of attacker and record their activities and actions. These are the real machine with one system, with one network interface on network. An example of this type of honeypot is *Honeynet.* [1]

Honeynets:

Two or more honeypots on a network form a honeynet. Typically, a honeynet is used for monitoring a larger and/or more diverse network in which one honeypot may not be sufficient. Honeynets and honeypots are usually implemented as parts of larger network intrusion detection systems. A honeyfarm is a centralized collection of honeypots and analysis tools. [11]

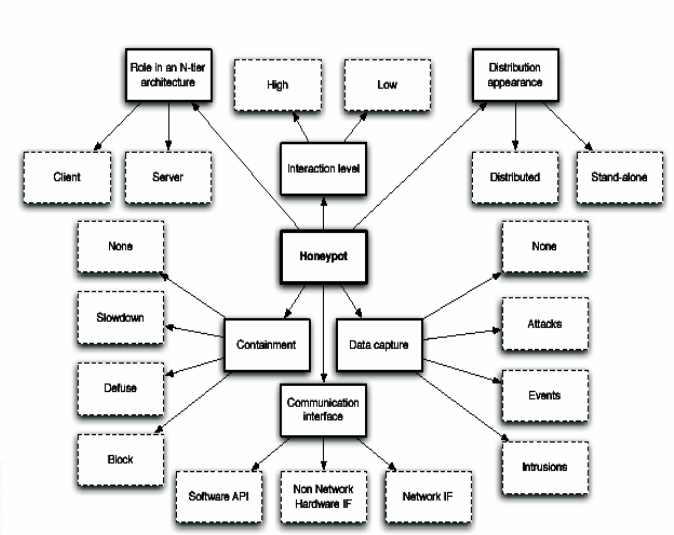

Figure 1: Taxonomy of Honeypot: From Urjita Thakar, Sudarshan Varma, A.K. Ramani (2005).

III. HONEPOT FOR SMALL SCALE INDUSTRIES

Honeypot that is designed for the small scale industry keep information of the complete networking system, keep the records of all log files of the network. The complete attacker's information is gathered and recorded all the activities. The honeypot for small scale industry is implemented by configuring the 2 or 3 tools together. These tools are used for the information gathering of the attackers. Sniffing is prevented with the help of these tools. Packets can be logged that are coming across our network. It can be used for the port scanning as to know the open and closed ports. Virtual computer can be operated for providing the fake information to the attacker. [2]

A set of services are simulated on the network, so as the honeypot should look like a real machine to the attacker. These services are:-

- HTTP
- POP3
- FTP
- TELNET

So these are the main services where the honeypot can work for and provide the security for the network from the hackers.

In the proposed architecture, I have used the various tools for the intrusion detection and noticing the activities of attacker and to make the real system safe. The attacker will attack on the virtual machine and honeypot will capture all activities and behavior of the attacker.

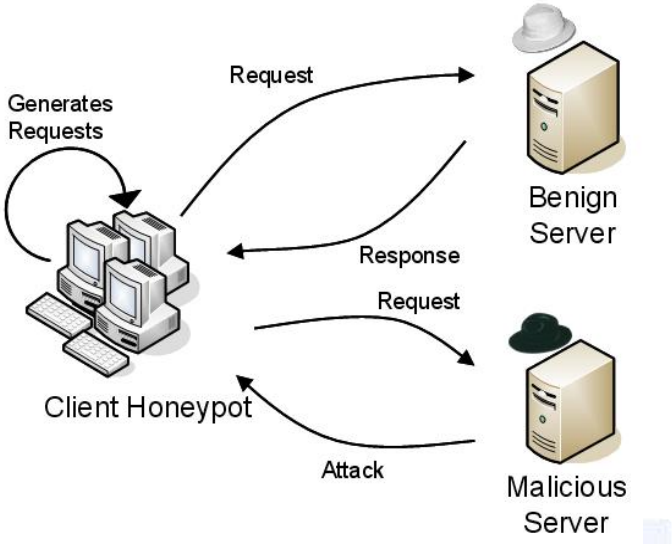

Figure 2: - Honeypot Architecture: From C K Shyamala, N Harini, Dr T R Padomanabhan (2011).

IV. OBJECTIVE OF HONEYPOT

The main objective of the honeypot is to find the attacker by the **connection tracking** or the **pattern flow detection** technique. After then confuse the attacker that the attacker is spoofing the information from the legitimate user, but actually that was not the legitimate user, originally that was the duplicate or the false computer where the attacker attack the information. So objective of honeypot to confuse the attackers.

Now we will discuss the objective of the various types of honeypots. Here the production honeypots are used to help reduce risk and diverting hackers from attacking the production systems whereas a research honeypot is used to collect as much information and evidence as possible about the blackhat community. The latter may not bring any value on security to the organization but it sure helps an organization to understand the hacking techniques and tools used by hackers, attack patterns, how the blackhat community communicate with Internet.

This will later help the organization to build stronger defences for their internal IT infrastructure in their fight against hackers. Organizations have to deem all traffic to the honeypot as suspicious activity because there should not be any illegitimate traffic such as FTP and TELNET to and from this part of the network [11]. Data that is collected from the honeypot is of high value and can definitely lead to clearer comprehension to increase the security of an organization's IT environment. Depending on where the honeypot is placed, it will either collect vast amount of information that can be

overwhelming, but most of it will be redundant and useless to the organization, and on the other hand, it collects very little data, but can be of very high value. Any data collected can be a scan, probe or attack which are useful information to the organization. Sometimes, the probability of finding a honeypot in the network can be quite low as it does not have any production activity, thus does not generate high noise level. Depending on the honeypot tools used, useful information can be understood by the administrator from the easy-to-use graphical user interface. Data, especially those of malicious activity, can be used for statistical modelling, trend analysis, detecting attacks, or even researching attackers. Depending on the placement of the honeypot, and if they collect little data and monitor little activity, they will not have problems of resource exhaustion. [4]

Now the some of the other main objective of using the honeypot for the Intrusion Detection environment so that the computer network become secure from the intruder or the hacker attack described as below:-

Network decoys:
Honeypots are useful for monitoring networks. For monitoring, honeypots are deployed in such parts of a network that are not used for production. When an attacker probes the network, some traffic should eventually hit one of the honeypots. As normal traffic should not arrive at honeypots, warnings are rather reliable. However, honeypots are useless if the attacker is aware of them. Neither can they detect the absence of attacks. Besides of network monitoring, honeypots can be used for confusing attackers by implementing decoy systems. The attacker might not be able to tell which systems have real value and which do not. Because of this, the attacker may have to work harder and use more time targeting the system. This makes detection easier. Nevertheless, the setup of plausible decoys can be rather tedious, and they involve risk, as well. So this about the network decoy to protect the system from the intruder or the unauthorized user means hacker.

Prevention of spam:
Spammers abuse *open mail relays* and *open proxies* to hide their identity [4]. An open mail relay accepts any sender without authentication to send mail further. Open proxies accept any client in the network to make connections through it. Honeypots masquerading as open mail relays or open proxies can be used to capture spam and reveal its sources. Captured spam makes it possible to improve filtering. Knowing a source of spam might allow switching off the spammer from the network. Alternatively, a honeypot can collect source addresses of attempted mail deliveries. The addresses are temporarily added into the actual mail server's blacklist. This helps to filter out sources that almost certainly try to send spam. Honeypots seem to have been effective to some extent since spammers have developed methods to detect false open proxies. A simple test is to try to send mail back to itself by the proxy. The proxy is very likely a honeypot if it claims a success, but in reality the message has not come back. The test is relatively simple to counter, however. The honeypot has only to compare the source and destination addresses and let the connection through if they are the same. A more complicated test would place the sender and receiver on different hosts. In a general setting, this is much more difficult to cope without being detected as the honeypot should not be a real open proxy. Unfortunately, honeypots are probably less effective against spam sent using botnets than by open mail relays and open proxies [8]. A botnet's controller is presumably carefully hidden and can not be figured out from spam delivery attempts. In addition, blacklisting attempts are not very useful either, since there are so many potential senders.

Collecting malware:
A suitable honeypot can automatically collect samples of malware that spread autonomously. This allows large-scale capture of currently active malware. This in turn allows, for example, research on live data and constant refinement of intrusion detection and antivirus software [11]. Manual capture of malware would be just too slow. The objective of a malware-collecting honeypot is essentially to download the actual malware and record the details of that event. When a network connection might lead to an exploit, the honeypot captures the connection's payload. It is then analysed whether the payload contains machine executable code or network addresses. If enough information is found, the honeypot downloads the possible malware. Low-interaction honeypots can, at least in principle, capture only malware that exploit known vulnerabilities since they rely on emulation. More comprehensive capture requires a high-interaction honeypot which runs a real operating system. [4]

Detection of malicious Web content:
Vulnerabilities in Web browsers might allow malicious Web pages to install malware into the system. Exploited pages are rather common nowadays, and thus their manual detection and analysis is not practical. Client honeypots can automate detection at least partially and help out in analysis. *HoneyMonkey* is a high-interaction client honeypot for detecting exploits [11]. The system consists of a set of Windows XP instances with different levels of patches running in virtual machines. The system is given a list of URLs that a modified Web browser within a virtual machine visits one by one. Between the URL visits, the state of the system, files and registry, is checked. If there were any modifications outside the browser's working area, the URL would be reported as an exploit and marked for further analysis. In that case, the exploited virtual machine instance is discarded and a clean one is started. So this is the main objective of the honeypot for the inrusion detection system. So we have studied the all the objectives in detail to protect the system from the intruder or the attacker.

V. WORKING METHODOLOGY

i. Data Capture / Traffic logging Components: - This part includes Honeyd and Tcpdump for data collection.

ii. Data analysis / analysis and extraction components: - This part contains data analysis part of signature extraction mechanism for extracting precise attack signature.

iii. Signature Extraction: - Steps to extract our good quality attack signatures. The signature extraction also used for describe the various attack signatures.

i. Data Capture: - The purpose of data capture is to log all the activities of an attacker. The Honeypot does exactly this that it collects information. The HoneyAnalyzer System Has two sources of data: Honeypot log and network traffic log from Tcpdump. The Honeyd framework supports several ways of logging network activity. It can create connections logs that reports attempted and computed connections for all protocols. But to analyze the complete attack scenario, the system need full payload of the packet entering and leaving the honeypot. This task is performed by the second element that is Tcpdump which captures every packet full payload. Tcpdump is a tool for network monitoring and one of the well known sniffers for Linux. It then dumps packets header information in the log file.

ii. Data Analysis: - In order to extract the more precise attack signature, a data analyzer has been developed as shown:-

1. The web interface gives a graphical output using the which security administrator can easily find out most attacked port, So these are the IP address to detect the location of the attacker or hacker. The proposed method of realization of the HoneyAnalyzer for extracting more precise attack signature is described below:-

i. Configure honeyd to simulate network.

ii. Run Tcpdump for traffic analysis.
iii. Invoke the auto run shell script that will run in a particular time interval and execute the parser utility that will parse the data from the honeyd log file and insert into the database. The realization of the parser utility can be done in any language, which has strong string tokenization capability like java.

iv. Execute the auto-run shell-script to push the honeyd logs data into the database. This will invoked by the cron.

v. Login to the web interface to view the attack patterns and analyse the data for extraction of good quality signature.

To enable the Security Administrator to select the suspicious data, the web GUI has the following features: -

i) Ability to display packet information from the database.

ii) Ability to display real time network traffic from data stored in database, as well as historical traffic statistics.

iii) Display the ports, which were attacked within a certain time range.

v) Now here the main scenario which remote IP-addresses were "visited" by Honeypot in a certain time range. Here it's possible to specify a port number to show activity on a specific port.

vi) A textual hit statistic over a certain time range. By specifying an IP or a port number it is possible to focus on specific events.

iii. Signature Extraction: - The graphical interface has support for application of LCS algorithm the data of interest while present system apply LCS algorithm on whole data. The process of finding attack signatures not fully automated rather it also depends upon security administrator's (SA) wisdom and experience. The SA can choose the traffic on which the LCS algorithm is to be applied. The Resulting precise signature will give less number of false positive and false negatives. The steps followed for finding the good quality attack signature are as follows:-

a. Identify the data of interest from the database by looking at the web GUI. This is the all about description about the signature extraction technique by detecting the intruder from the Graphic websites.

b. Analyze combined data from different data sources that is Honeypot and Tcpdump For each received packet initiate the following sequence of activities:-

i) Identify data of interest (i.e. of significance) from the database by looking at the web GUI.

ii) Analyze data from sources i.e. honeypot and Tcpdump.

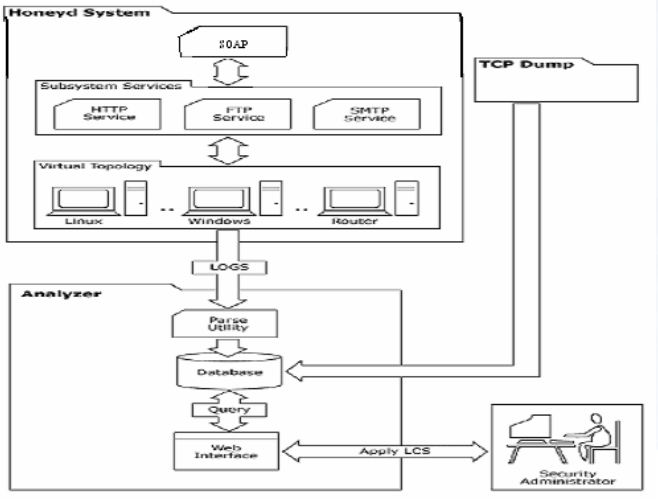

Figure 3: Honey Analyzer's architecture, illustrating honeyd as it is simulating a number of different machines, each running a number of pre-configured services. The HoneyAnalyzer has hooked itself into the wire to see in and outgoing connections and providing the web-interface: From Urjita Thakar, Sudarshan Varma, A.K. Ramani (2005).

a) If there is any existing connection state for the new packet, that state is updated otherwise new state is created.

b) If the packet is outbound, don't process the packet.

c) Perform protocol analysis [7] at the network and transport layer.

d) Each stored connection, perform header comparison to detect matching IP networks, TCP sequence numbers, etc.

iii) Apply content-based string matching algorithm on the payload of interest by applying following of activities:

a) If the connections have the same destination port, perform pattern detection on the exchanged messages with the help of Longest Common Substring algorithm. A description about string based pattern detection is given in the [9].

b) If a new signature is created in the process use the signature to augment the signature pool otherwise stop the process.

VI. COMPARISON OF HONEYANALYZER /HONEYCOMB

i) Pairwise LCS employed by Honeycomb often leads to redundant (non-identical) signatures, which would generate multiple alarms for the same attack. While, HoneyAnalyzer generalizes the approach such that a security administrator who is aware of protocol semantics can groom the signature to Make it far less prone to redundant signature production.

ii) Honeycomb's lack of semantics awareness leads to signatures consisting of benign sub strings. These lead to false positives, thus Honeycomb is unable to produce precise signatures for protocols such as NetBIOS, MS-SQL and HTTP attacks, such as Nimda [10], where the exploit content is a small portion of the entire attack string. In case of HoneyAnalyzer semantics awareness is the responsibility of security administrator. He can better understand the benign substrings of the local network and can filter out redundant and useless strings.

Thus the signatures obtained through HoneyAnalyzer are of high quality and result in more precise intrusion detection. HoneyAnalyzer can also act as an intrusion indicator i.e. how, when and from where different intrusion attempts are taking place. This can be shown through the graphical interface. Honeypots are increasingly deployed in networks; however, they are mostly used passively and administrators watch it just for what happens. The proposed system gives better control to the security administrator on intrusion detection process for Extracting good quality attack signature.

VII. ADVANTAGES / DISADVANTAGES

There are various advantages and the disadvantages for using the honeypot so that the network system becomes secure and protected from the outsider attacker or hacker. Now some of advantages and disadvantages as below:-

Advantages of honeypots:

There are many security solutions available in the market. Anyone can browse the variety of choices through internet and find the most suitable solution for their needs. Here are the reasons why I should choose honeypots. Honeypots can capture attacks and give information about the attack type and if needed, thanks to the logs, it is possible to see additional information about the attack. New attacks can be seen and new security solutions can be created by looking at them. More examinations can be obtained by looking at the type of the malicious behaviors. It helps to understand more attacks that may happen. Capturing data. They are only dealing with the incoming malicious traffic. Therefore, the information that has been caught is not as much as the whole traffic. Focusing only on the malicious traffic makes the investigation far easier. Therefore, this makes honeypots very useful. For the only malicious traffic, there is no need for huge data storage. There is no need for new technology to maintain. Any computer can be used as a honeypot system. Thus, it does not cost additional budget to create such a system. They are simple to understand, to configure and to install. They do not have complex algorithms [4]. There is no need for updating or changing some things. As honeypots can capture anything malicious, it can also capture new tools for detecting attacks too. It gives more ideas and deepness of the subject proving that it is possible to discover different point of views and apply them for our security solutions.

Disadvantages of honeypots:

As there are several important advantages of using honeypots, there are also some disadvantages of them as well. You can only capture data when the hacker is attacking the system actively. If he does not attack the system, it is not possible to catch information. If there is an attack occurring in another system, the honeypot will not be able to identify it. So, attacks not towards the honeypot system may damage other systems and cause big problems. There is fingerprinting disadvantage of honeypots. It is easy for an experienced hacker to understand if he is attacking a honeypot system or a real system. Fingerprinting allows to distinguish between these two. It is a not a wanted result of the experiment [4]. The honeypot may be used as a zombie to reach other systems and compromise them. This can be very dangerous.

VIII. PROBLEM DEFINATION

In this report I have discussed the various Types of Intruder attack that can be occurred on the web services. And also discuss the tool that is Honeypot for the Intruder Detecting services and discuss the various effects of the intruder attack on the web services. I have also discussed the Introduction and the working environment on which the Honeypot can work to detect the various types of Intruder attack on the web services. But the problem is that to make the Honeypot and the HoneyAnalyzer more flexible, certain more parameters like allowing the negative interpretation of input. The problem is also that the comparison between the existing method and the proposed method should also have to be done. Also there should be the need of the implementations of the some algorithms and the techniques like connection tracking, protocol analysis and the pattern detection and the flow

content based on which the security administrator can perform the analysis and extract the signature with even greater precision [8]. There is also the need of the some more advantages and the disadvantages of the Honeypot should also have to be discussed. The working environment of the Honeypot in which to detect the various intruder attacks should also have to be made more flexible so that the recent types of intruder attacker on the web services should also be detected.

IX. CONCLUSION

Honeypot is not a solution to network security but a good tool supplements other security technologies to form an alternative active defense system for network security. Working with **IDS** and firewall, Honeypot provides new way to attacks prevention, detection and reaction. Honeypot can serve **as** a good deception tool for prevention of product system because of its ability of trapping attacker to a decoy system. Supplemented with IDS, honeypot reduces false positives and false negatives. Intelligence routing control provides flexible response to attacks. Different kinds of honeypot share the common technologies of data control and data capture. Experts focus the two to make honeypot easier to deploy and more difficult to detect. From the advances in research and production honeypot now days, I predict the future honeypot has the features of integration, virtualization and distribution. Integrated honeypot encapsulates all the components in **a** single device. Virtual honeypot creates large number of honeypot systems in one machine. Distributed honeypot comprises different honeypot system in an actual network to offer high interaction between **attacks and** system. **All** of them make future honeypot cheaper to apply and easier to maintain.

X. FUTURE WORK

In the future, attempt can be made to add implementation of some more algorithms and techniques like connection tracking, protocol analysis, and pattern detection in flow content etc. based on which security administrator can perform the analysis and extract the signature with even greater precision [8]. To make HoneyAnalyzer more flexible, certain more parameters like allowing the negative interpretation of input like Port! = 445 that will show activities on all Ports except 445 can also be added. A quantitative comparison also needs to be done between the existing method and proposed method to illustrate the advantages of proposed system over existing system.

REFERENCES

[1] R.Baumann, C.Plattner "honeypots" Diploma Thesis in Computer Science, 2002.
[2] Gurleen Singh., Sakshi Sharma, Prabhdeep Singh "Design and develop a Honeypot for small scale organization "in IJITEE. Vol 2, issue-3, Feb2013.
[3] H.Artail, H.Safa, M.Sraj, I.Kuwalty, Z.Masri "A hybrid honeypot framework for improving intrusion detection systems in protecting organizational networks" Science Direct, 2006.
[4] Deniz Akkaya – Fabien Thalgott, "Network Security Using Honeypot" IEEE, June 2010.
[5] Y.K.Jain, S. Singh "Honeypot based Secure Network System" in IJCSE. Vol 3. No.2 Feb 2011.
[6] S. Mrdovic, E. Zajko "Secured Intrusion Detection System Infrastructure", ICAT 2005.
[7] Erwan Lemonnier, Defcom, "Protocol Anomaly Detection in Network-based IDSs", http://erwan.lemonnier.free.fr/.
[8] Urjita Thakar, Sudarshan Varma, A.K. Ramani " HoneyAnalyzer – Analysis and Extraction of Intrusion Detection Patterns & Signatures Using Honeypot" in Second International Conference on Innovations in Information Technology (IIT'05) Dubai, UAE September 26-28, 2005.
[9] Hyang-Ah Kim, Brad Karp, "Autograph: Toward Automated, Distributed Worm Signature Detection," In Proceedings of the 13th Usenix Security Symposium, San Diego, CA, August 2004. Pp. 271–286.
[10] Christian Kreibich, Jon Crowcroft, "Honeycomb-Creating Intrusion Detection Signatures" Using Honeypot, ACM SIGCOMM Computer Communication Review archive Volume 34,Issue1 January 2004, Pp. 51 – 56.
[11] C K Shyamala, N Harini, Dr T R Padomanabhan – Cryptography and Security, May 2011.