Volume 8, No. 3, March – April 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
REVIEW ARTICLE
Available Online at www.ijarcs.info

A Review on Recent Advances & Future Trends of Security in Honeypot

Praveen Kumar
M. Tech CS
Department of Computer Science
BBAU ,Lucknow, U.P., India

Ram Singar Verma
Assistant Professor
Department of Computer Science
BBAU ,Lucknow, U.P., India

***Abstract*:** PC Network and Internet is developing each day. PC systems permit conveying speedier than whatever other offices. These systems permit the client to get to neighborhood and remote databases. It is difficult to secure each framework on the system. In businesses, the system and its security are essential issues, as a break in the framework can bring about real issues. Interruption location framework (IDS) is utilized for observing the procedures on a framework or a system for looking at the dangers and alarms the head about assault. Also, IDS give an answer just to the expansive scale businesses, however there is no answer for the little scale ventures so model is proposed for honeypot to take care of the issue of little scale enterprises which is the half and half structure of Snort, Nmap, Xprobe2, and P0f [1]. This model catches the exercises of aggressors and keeps up a log for every one of these exercises. Virtualization is performed with the assistance of virtual machine. The concentration of this report is essentially on keeping the assaults from outer and inside assailants and keeping up the log record utilizing honeypot with virtual machine [2].

***Keywords*:** Intrusion detection system, honeypots, attacker, security.

I. INTRODUCTION

Size of Internet innovation is substantial and it is as yet developing each day. The security of system is required for development of the ventures which are subject to the web to upgrade the business and giving administrations on the system. So security of system is essential worry of the businesses for securing the basic data. Huge aggregates of assaults are seen as of late on these sorts of enterprises. Interruption identification framework (IDS) is utilized for observing the procedures on a framework or a system for looking at the dangers and caution the head. IDS and firewalls are utilized for shielding the framework and system from assaults, however after such a variety of endeavors for security still the system is not completely secured so extraordinary sorts of arrangements are proposed by the specialists.

The little scale businesses utilizing LAN need to keep high their own security level as the database, server and customers are altogether taken care of independent from anyone else. Since danger from interior system is Always the huge test for the heads, so an answer is required for little scale system to secure their inner system. This report gives the answer for a similar utilizing honeypot.

II. LITERATURE REVIEW

Honeypot is a non-creation framework, utilized for abusing the assailant and notice the assaulting strategies and activities. The target of honeypots is to see as well as to handle the hazard and expel it. There are different meanings of honeypots are accessible as few individuals take it as a framework to befuddle the aggressors and assess their exercises where as other take it as an innovation for distinguishing assaults or genuine frameworks shaped for getting assaulted.
In system security, honeypots are utilized to recognize the assailants and gain from their assaults and after that change and build up the framework as needs be for security. The escape clauses of the system security can be secured with the assistance of data gave by honeypots.
Honeypot can be figured as a PC framework associated with a system for investigating the vulnerabilities of a PC or an entire system. The escape clauses can be inspected on the whole or separately of any framework, as it is a selective apparatus to learn about the assailants and their methodologies on the system. [3]
Honeypots are ordinarily virtual machines which acts like a genuine framework. Honeypots are ordered into taking after classes on their utilization:

Research honeypots:

These are the honeypots which are controlled and are utilized to secure data and learning of the programmer society. The information picked up by the specialists are utilized for the early notices, judgment of assaults, improve the interruption discovery frameworks and outlining better devices for security.

Production honeypots:

These are the honeypots determined by the enterprises as a piece of system security spine. These honeypots fills in as early cautioning frameworks. The destinations of these honeypots are to expel the dangers in enterprises. It gives the data to the manager before the genuine assault. [1] [4]

Honeypots can likewise be grouped on the premise of level of contribution or collaboration as:

Low level interaction:

Honeypots that give just some fake administrations, these goes about as an emulator of the working framework and administrations. These honeypots are easy to outline additionally just perceivable. Aggressor can simply utilize a straightforward charge to recognize it that a low association

honeypot does not bolster. A case of this kind of honeypot is Honeyd.

High level interaction:

Abnormal state connection honeypots gives the genuine like working frameworks and some genuine administrations with some genuine instabilities. These permit the catching of data of aggressor and record their exercises and activities. These are the genuine machine with one framework, with one system interface on system. A case of this kind of honeypot is Honeynet. [1]

Honeynets:

At least two honeypots on a system shape a honeynet. Normally, a honeynet is utilized for observing a bigger or potentially more differing system in which one honeypot may not be adequate. Honeynets and honeypots are normally executed as parts of bigger system interruption recognition frameworks. A honeyfarm is a concentrated gathering of honeypots and investigation apparatuses. [11]

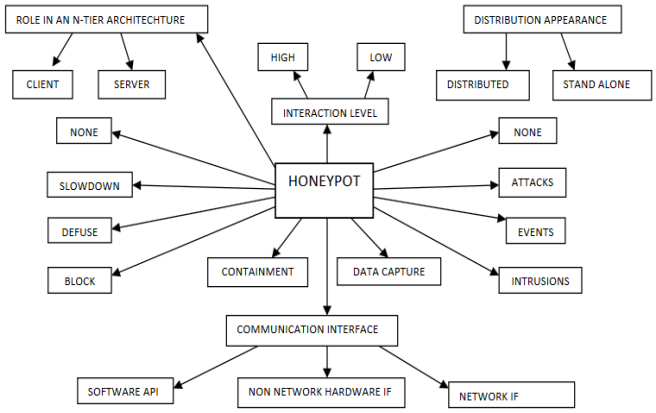

Figure 1: Taxonomy of Honeypot

III. HONEPOT FOR SMALL SCALE INDUSTRIES

Honeypot that is intended for the little scale industry keep data of the entire systems administration framework, keep the records of all log documents of the system. The total aggressor's data is assembled and recorded every one of the exercises. The honeypot for little scale industry is executed by designing the 2 or 3 instruments together. These apparatuses are utilized for the data social occasion of the aggressors. Sniffing is anticipated with the assistance of these apparatuses. Bundles can be logged that are running over our system. It can be utilized for the port filtering as to know the open and shut ports. Virtual PC can be worked for giving the fake data to the aggressor. [2] An arrangement of administrations are recreated on the system, so as the honeypot ought to resemble a genuine machine to the aggressor. These administrations are:-

So these are the principle administrations where the honeypot can work for and give the security to the system from the programmers.

- HTTP
- POP3
- FTP
- TELNET

In the proposed engineering, I have utilized the different devices for the interruption discovery and seeing the exercises of assailant and to make the genuine framework safe. The assailant will assault on the virtual machine and honeypot will catch all exercises and conduct of the aggressor.

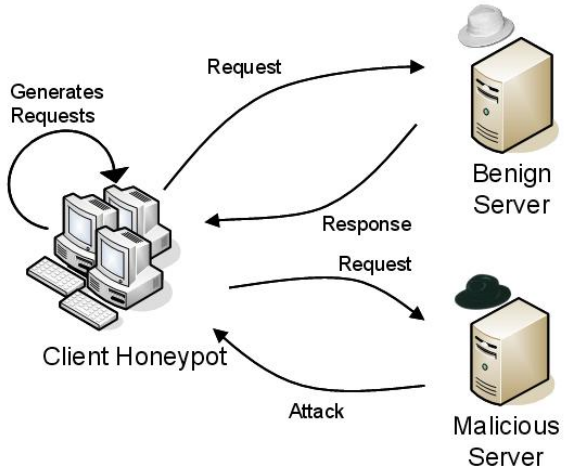

Figure 2: - Honeypot Architecture:

IV. OBJECTIVE OF HONEYPOT

The principle target of the honeypot is to discover the aggressor by the association following or the example stream identification procedure. After then befuddle the aggressor that the assailant is mocking the data from the true blue client, all things considered that was not the genuine client, initially that was the copy or the false PC where the assailant assault the data. So target of honeypot to befuddle the aggressors.

Presently we will talk about the goal of the different sorts of honeypots. Here the generation honeypots are utilized to offer assistance decrease chance and redirecting programmers from assaulting the generation frameworks while an examination honeypot is utilized to gather however much data and confirmation as could reasonably be expected about the blackhat group. The last may not bring any esteem on security to the association yet it beyond any doubt helps an association to comprehend the hacking strategies and apparatuses utilized by programmers, assault designs, how the blackhat group speak with Internet. This will later help the association to manufacture more grounded resistances for their inward IT foundation in their battle against programmers.

Associations need to consider all movement to the honeypot as suspicious action in light of the fact that there ought not be any ill-conceived activity, for example, FTP and TELNET to and from this some portion of the system [5]. Information that is gathered from the honeypot is of high esteem and can prompt clearer appreciation to build the security of an association's IT condition. Contingent upon where the honeypot is put, it

will either gather inconceivable measure of data that can be overpowering, yet the majority of it will be repetitive and futile to the association, and then again, it gathers next to no information, yet can be of high esteem. Any information gathered can be a sweep, test or assault which are helpful data to the association. Now and then, the likelihood of finding a honeypot in the system can be very low as it doesn't have any creation movement, subsequently does not

produce high commotion level. Contingent upon the honeypot apparatuses utilized, helpful data can be comprehended by the chairman from the simple to-utilize graphical UI. Information, particularly those of malevolent movement, can be utilized for measurable demonstrating, incline examination, distinguishing assaults, or notwithstanding investigating aggressors. Contingent upon the position of the honeypot, and in the event that they gather little information and screen little action, they won't have issues of asset fatigue. [4]

Presently the a portion of the other primary goal of utilizing the honeypot for the Intrusion Detection condition so that the PC organize end up plainly secure from the interloper or the programmer assault depicted as beneath:-

Network decoys:

Honeypots are helpful for observing systems. For observing, honeypots are conveyed in such parts of a system that are not utilized for creation. At the point when an assailant tests the system, some movement ought to in the long run hit one of the honeypots. As typical movement ought not land at honeypots, notices are somewhat dependable. Be that as it may, honeypots are pointless if the assailant knows about them. Neither would they be able to identify the nonattendance of assaults. Other than of system checking, honeypots can be utilized for befuddling aggressors by actualizing imitation frameworks. The aggressor won't not have the capacity to tell which frameworks have genuine esteem and which don't. Along these lines, the aggressor may need to work harder and utilize additional time focusing on the framework. This makes recognition simpler. By and by, the setup of conceivable distractions can be somewhat dreary, and they include chance, also. So this about the system distraction to shield the framework from the interloper or the unapproved client implies programmer.

Prevention of spam:

Spammers manhandle open mail transfers and open intermediaries to shroud their character [4]. An open mail hand-off acknowledges any sender without verification to send letters promote. Open intermediaries acknowledge any customer in the system to make associations through it. Honeypots taking on the appearance of open mail transfers or open intermediaries can be utilized to catch spam and uncover its sources. Caught spam makes it conceivable to enhance sifting. Knowing a wellspring of spam may permit turning off the spammer from the system. Then again, a honeypot can gather source locations of endeavored mail conveyances. The locations are incidentally included into the genuine mail server's boycott. This channels out sources that in all likelihood attempt to send spam. Honeypots appear to have been compelling to some degree since spammers have created strategies to distinguish false open intermediaries. A straightforward test is to attempt to send letters back to itself by the intermediary. The intermediary is likely a honeypot on the off chance that it guarantees a win, yet in all actuality the message has not returned. The test is generally easy to counter, be that as it may. The honeypot has just to analyze the source and goal addresses and let the association through on the off chance that they are the same. A more muddled test would put the sender and beneficiary on various hosts. In a general setting, this is considerably more hard to adapt without being identified as the honeypot ought not be a genuine open intermediary. Shockingly, honeypots are likely less successful against spam sent utilizing botnets than by open mail transfers and open intermediaries [6]. A botnet's controller is apparently deliberately covered up and can not be made sense of from spam conveyance endeavors. Also, boycotting endeavors are not exceptionally valuable either, since there are such a variety of potential senders.

Collecting malware:

A reasonable honeypot can naturally gather tests of malware that spread self-governingly. This permits expansive scale catch of presently dynamic malware. This thus permits, for instance, look into on live information and steady refinement of interruption identification and antivirus programming [7]. Manual catch of malware would be quite recently too moderate. The goal of a malware-gathering honeypot is basically to download the real malware and record the points of interest of that occasion. At the point when a system association may prompt an endeavor, the honeypot catches the association's payload. It is then dissected whether the payload contains machine executable code or system addresses. In the event that enough data is found, the honeypot downloads the conceivable malware. Low-connection honeypots can, in any event on a basic level, catch just malware that adventure known vulnerabilities since they depend on imitating. More complete catch requires a high-cooperation honeypot which runs a genuine working framework. [4] relatively easy to counter, be that as it may. The honeypot has just to think about the source and goal addresses and let the association through on the off chance that they are the same. A more convoluted test would put the sender and recipient on various hosts. In a general setting, this is considerably more hard to adapt without being identified as the honeypot ought not be a genuine open intermediary. Lamentably, honeypots are likely less viable against spam sent utilizing botnets than by open mail transfers and open intermediaries [8]. A botnet's controller is probably deliberately covered up and can not be made sense of from spam conveyance endeavors. Furthermore, boycotting endeavors are not exceptionally valuable either, since there are such a variety of potential senders.

Detection of malicious Web content:

Vulnerabilities in Web programs may permit malevolent Web pages to introduce malware into the framework. Abused pages are fairly basic these days, and in this way their manual identification and examination is not commonsense. Customer honeypots can computerize discovery in any event incompletely and assist in examination. HoneyMonkey is a high-communication customer honeypot for identifying misuses [9]. The framework comprises of an arrangement of Windows XP cases with various levels of patches running in virtual machines. The framework is given a rundown of URLs that a changed Web program inside a virtual machine visits one by one. Between the URL visits, the condition of the framework, documents and registry, is checked. In the event that there were any alterations outside the program's working range, the URL would be accounted for as an endeavor and set apart for further investigation. All things considered, the abused virtual machine occurrence is disposed of and a perfect one is begun. So this is the principle target of the honeypot for the inrusion discovery framework. So we have concentrated the every one of the

targets in detail to shield the framework from the gatecrasher or the assailant.

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 motivation behind information catch is to log every one of the exercises of an assailant. The Honeypot does precisely this that it gathers data. The HoneyAnalyzer System Has two wellsprings of information: Honeypot log and system movement log from Tcpdump. The Honeyd structure bolsters a few methods for logging system action. It can make associations logs that reports endeavored and registered associations for all conventions. However, to dissect the total assault situation, the framework require full payload of the parcel entering and leaving the honeypot. This errand is performed by the second component that is Tcpdump which catches each bundle full payload. Tcpdump is an instrument for system checking and one of the well known sniffers for Linux. It then dumps bundles header.
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 yield utilizing the which security executive can without much of a stretch discover most assaulted port, So these are the IP deliver to distinguish the area of the aggressor or programmer. The proposed strategy for acknowledgment of the HoneyAnalyzer for extricating more exact assault mark is depicted beneath:-
i. Configure honeyd to simulate network.
ii. Run Tcpdump for traffic analysis.
iii. Conjure the auto run shell script that will keep running in a specific time interim and execute the parser utility that will parse the information from the honeyd log document and embed into the database. The acknowledgment of the parser utility should be possible in any dialect, which has solid string tokenization capacity like java.
iv. Execute the auto-run shell-script to push the honeyd logs information into the database. This will summoned by the cron.
v. Login to the web interface to see the assault designs and break down the information for extraction of good quality mark. To empower the Security Manager to choose the suspicious information, the web GUI has the accompanying elements: -
i) Capacity to show bundle data from the database.
ii) Capacity to show ongoing system movement from information put away in database, and verifiable activity insights.
iii) Show the ports, which were assaulted inside a certain time run.
v) Now here the principle situation which remote IP-addresses were "went by" by Honeypot in a specific time extend. Here it's conceivable to determine a port number to show movement on a particular port.
vi) A literary hit measurement over a specific time run. By determining an IP or a port number it is conceivable to concentrate on particular occasions.
iii. Signature Extraction: -
The graphical interface has bolster for utilization of LCS calculation the information of intrigue while exhibit framework apply LCS calculation on entire information. The way toward discovering assault marks not completely computerized rather it additionally relies on security executive's (SA) insight and experience. The SA can pick the movement on which the LCS calculation is to be connected. The Subsequent exact mark will give less number of false positive and false negatives. The means took after for finding the great quality assault mark are as per the following:-

a. Recognize the information of enthusiasm from the database by taking a gander at the web GUI. This is the about portrayal about the signature extraction procedure by identifying the interloper from the Realistic sites.
b. Examine joined information from various information sources that is Honeypot and Tcpdump For each got parcel start the taking after succession of exercises:-
i) Distinguish information of intrigue (i.e. of centrality) from the database by taking a gander at the web GUI.
ii) Investigate information from sources i.e. honeypot and Tcpdump.

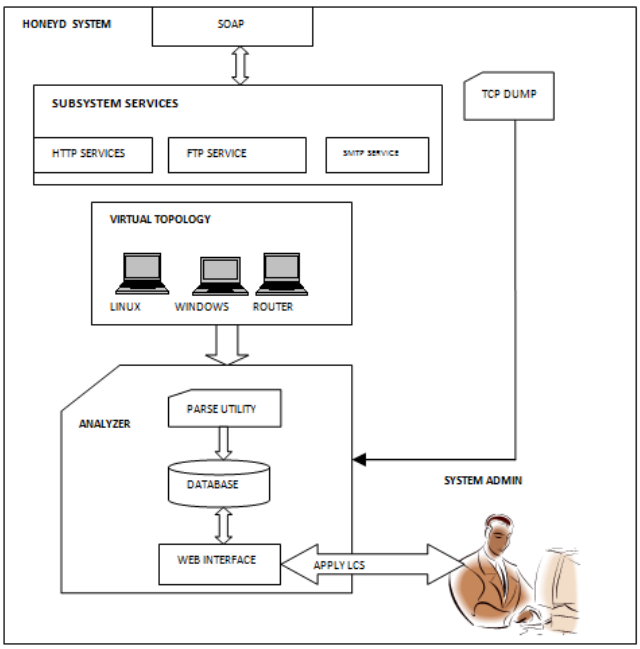

Figure 3: Honey Analyzer's architecture, illustrating honeyd as it is simulating a number of different machines, each running a number of pre-configured services.

The HoneyAnalyzer has hooked itself into the wire to see in and outgoing connections and providing the web-interface:
a) If there is any current association state for the new packet,that state is refreshed generally new state is made.
b) If the bundle is outbound, don't handle the parcel.
c) Perform convention examination [7] at the system and transport layer.

d) Each put away association, perform header correlation with distinguish coordinating IP systems, TCP grouping numbers, and so on.

iii) Apply content-construct string coordinating calculation in light of the payload of enthusiasm by applying taking after of exercises:

a) If the associations have a similar goal port, perform design recognition on the traded messages with the assistance of Longest Normal Substring calculation. A portrayal about string based example recognition is given in the [9].

b) If another mark is made in the process utilize the mark to increase the mark pool generally stop the procedure.

VI. COMPARISON OF HONEY ANALYZER

i) Pairwise LCS utilized by Honeycomb frequently prompts excess (non-indistinguishable) marks, which would create various alerts for a similar assault. While, HoneyAnalyzer sums up the approach with the end goal that a security executive who knows about convention semantics can prep the mark to Make it far less inclined to excess mark creation.

ii) Honeycomb's absence of semantics mindfulness prompts marks comprising of benevolent sub strings. These prompt false positives, consequently Honeycomb can't deliver exact marks for conventions, for example, NetBIOS, MS-SQL and HTTP assaults, for example, Nimda [10], where the endeavor substance is a little bit of the whole assault string. If there should arise an occurrence of HoneyAnalyzer semantics mindfulness is the obligation of security executive. He can better comprehend the considerate substrings of the nearby system and can sift through repetitive and futile strings.

Subsequently the marks got through HoneyAnalyzer are of high caliber and result in more exact interruption location. HoneyAnalyzer can likewise go about as an interruption marker i.e. how, when and from where distinctive interruption endeavors are occurring. This can be appeared through the graphical interface. Honeypots are progressively conveyed in systems; in any case, they are generally utilized inactively and chairmen watch it only for what happens[11]. The proposed framework gives better control to the security chairman on interruption location prepare for Extricating great quality assault signature.

VII. ADVANTAGES / DISADVANTAGES

There are different favorable circumstances and the burdens for utilizing the honeypot so that the system framework ends up noticeably secure and shielded from the pariah aggressor or programmer. Presently some of focal points and weaknesses as underneath:-

Advantages of honeypots:

There are numerous security arrangements accessible in the market. Anybody can peruse the assortment of decisions through web and locate the most reasonable answer for their requirements. Here are the reasons why I ought to pick honeypots. Honeypots can catch assaults and give data about the assault sort and if necessary, because of the logs, it is conceivable to see extra data about the assault. New assaults can be seen and new security arrangements can be made by taking a gander at them. More examinations can be acquired by taking a gander at the kind of the pernicious practices. It sees more assaults that may happen. Catching information. They are just managing the approaching malevolent activity. Hence, the data that has been gotten is not as much as the entire activity. Concentrating just on the pernicious activity makes the examination far less demanding. In this manner, this makes honeypots exceptionally valuable. For the main pernicious activity, there is no requirement for gigantic information stockpiling. There is no requirement for new innovation to keep up. Any PC can be utilized as a honeypot framework. In this way, it doesn't cost extra spending plan to make such a framework.

They are easy to comprehend, to design and to introduce. They don't have complex calculations [4]. There is no requirement for refreshing or changing a few things. As honeypots can catch anything noxious, it can likewise catch new apparatuses for identifying assaults as well. It gives more thoughts and profundity of the subject demonstrating that it is conceivable to find diverse purpose of perspectives and apply them for our security arrangements.

Disadvantages of honeypots:

As there are a few vital favorable circumstances of utilizing honeypots, there are a few hindrances of them also. You can just catch information when the programmer is assaulting the framework effectively. On the off chance that he doesn't assault the framework, it is unrealistic to catch data. In the event that there is an assault happening in another framework, the honeypot won't have the capacity to recognize it. In this way, assaults not towards the honeypot framework may harm different frameworks and cause enormous issues. There is fingerprinting inconvenience of honeypots. It is simple for an accomplished programmer to comprehend on the off chance that he is assaulting a honeypot framework or a genuine framework. Fingerprinting permits to recognize these two. It is a not a needed aftereffect of the examination [4]. The honeypot might be utilized as a zombie to achieve different frameworks and bargain them. This can be exceptionally unsafe.

VIII. PROBLEM DEFINATION

In this report I have talked about the different Sorts of Interloper assault that can be happened on the web administrations. And furthermore examine the apparatus that is Honeypot for the Gatecrasher Recognizing administrations and talk about the different impacts of the interloper assault on the web administrations. I have likewise examined the Presentation and the workplace on which the Honeypot can work to identify the different sorts of Interloper assault on the web administrations. In any case, the issue is that to make the Honeypot and the HoneyAnalyzer more adaptable, certain more parameters like permitting the negative understanding of information. The issue is likewise that the correlation between the current technique and the proposed strategy ought to likewise must be finished. Additionally there ought to be the need of the executions of the a few calculations and the systems like association following, convention investigation and the example discovery and the stream content in view of which the security executive can play out the examination and concentrate the mark with much more noteworthy accuracy [8]. There is likewise the need of the some more focal points and the drawbacks of the Honeypot ought to likewise must

be talked about. The workplace of the Honeypot in which to distinguish the different gatecrasher assaults ought to likewise must be made more adaptable so that the current sorts of interloper assailant on the web administrations ought to likewise be identified.

IX. CONCLUSION

Honeypot is not an answer for system security but rather a decent instrument supplements other security advances to shape an option dynamic guard framework for system security. Working with IDS and firewall, Honeypot gives better approach to assaults counteractive action, identification and response. Honeypot can fill in as a decent trickiness instrument for aversion of item framework as a result of its capacity of catching assailant to an imitation framework. Supplemented with IDS, honeypot lessens false positives and false negatives. Insight steering control gives adaptable reaction to assaults. Various types of honeypot share the normal advances of information control and information catch. Specialists center the two to make honeypot less demanding to send and more hard to identify. From the advances in research and generation honeypot now days, I foresee the future honeypot has the components of mix, virtualization and appropriation. Incorporated honeypot typifies every one of the parts in a solitary gadget. Virtual honeypot makes huge number of honeypot frameworks in one machine. Circulated honeypot includes diverse honeypot framework in a genuine system to offer high association amongst assaults and framework. Every one of them make future honeypot less expensive to apply and less demanding to keep up.

X. FUTURE WORK

Later on, endeavor can be made to include execution of some more calculations and strategies like association following, convention examination, and example recognition in stream content and so forth in light of which security overseer can play out the investigation and concentrate the mark with much more prominent accuracy [11].To make Honey Analyzer more adaptable, certain more parameters like permitting the negative elucidation of info like Port! = 445 that will indicate exercises on all Ports aside from 445 can likewise be included. A quantitative correlation additionally should be done between the current technique and proposed strategy to represent the upsides of proposed framework over existing framework.

REFERENCES

[1] 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.

[2] Y.K.Jain, S. Singh “Honeypot based Secure Network System” in IJCSE. Vol 3. No.2 Feb 2011.

[3] Gurleen Singh., Sakshi Sharma, Prabhdeep Singh “Design and develop a Honeypot for small scale organization “in IJITEE. Vol 2, issue-3, Feb2013.

[4] Deniz Akkaya – Fabien Thalgott, “Network Security Using Honeypot” IEEE, June 2010.

[5] R.Baumann, C.Plattner “honeypots” Diploma Thesis in Computer Science, 2002.

[6] Erwan Lemonnier, Defcom, “Protocol Anomaly Detection in Network-based IDSs”, http://erwan.lemonnier.free.fr/.

[7] S. Mrdovic, E. Zajko “Secured Intrusion Detection System Infrastructure”, ICAT 2005.

[8] 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.

[9] C K Shyamala, N Harini, Dr T R Padomanabhan – Cryptography and Security, May 2011.

[10] 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.

[11] 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.