A STUDY ON LOCAL NETWORK FOR DETECTION OF ATTACK USING HONEYNET

Rupinder Kaur[1], Er.Sunil Nagpal[2], Saurabh Chamotra[3]

[1] *M.Tech (CSE), Baba Farid College of Engineering and Technology, Bathinda, (India)*

[2] *Ph.D Research Scholar, Punjab Technical University, Computer Science Department, Kapurthala (India)*

[3] *Sr.Engg /Scientist C, CDAC, A-34 Phase 8 Industrial Area, Mohali, (India)*

ABSTRACT

In this paper we describes the honeynet that analysis network traffic for detection of attack. As per Wikipedia "a honeynet is a network, placed behind a reverse firewall that captures all inbound and outbound traffic. The reverse firewall limits the amount of malicious traffic that can leave the honeynet. The data is contained, captured, and controlled by honeynet. A user traffic profile is used to filter the normal traffic that is generated by the host. Remaining suspicious traffic is study to detailed analysis, nature of detailed analysis is derived from characterization of worm traffic. It is designed to detect unknown new attacks from the enterprise network. The high bandwidth usages on these networks make it very difficult to identify malicious traffic within the enterprise network. We propose that a Honeynet can be used to assist the system administrator in identifying malicious traffic on the enterprise network. In particularly we focus on issue of handling unknown traffic pattern with in our approach. Our assumption is that being to track the entire malware execution of compromised system of the attacker through there we can improve the security for our enterprise network.

Keywords: Internet Security, Honeynet, Worm Traffic Characterization, Unknown Traffic Reduction, Intrusion Detection System.

I.INTRODUCTION

As the organizations are more and more dependent on the network infrastructure and more complicated in network architecture to provide the necessary services and security against the compromised system of the intruder. The honeynet are exciting a new technology greater potential in security community. A fundamental challenge in this activity is determining how to select a target address. While many methods have been proposed, simply sending scans to all addresses in specified network. While this approach can be quite effective, it is also offers the network security community a significant opportunity for gathering detailed information on attack by deploying measurement systems on routed but otherwise unused IP addresses in a network segment [3]. These measurements are typically referred to as a honeynet. It is a sensitive technique for prevention and detection of attack or worms performed on a complex network, so there is reason for study of honeynet deployment in an enterprise network.The purpose of this is to detect and learn from attacks and use the information to improve the security. Honeynet are not a software solution that is installed on computer. Honeynet is architecture that entire network of computer designed to be attacked. This ideas is to have an architecture that creates a highly controlled network one where the all the activities of bad guy is controlled and captured through the honeynet.

II. HONEYNET & ITS REQUIREMENTS

Honeynet is trap that tracks the attackers which is attempting to compromise the information of organizational system. It is collection of multiple honeypot connected in a network to be appearing as a functioning network. It can be capture the extensive amount of information that is valuable for detect the attacks or worms from the enterprise network [10]. Honeynet is a network, placed behind the firewall that captures all inbound and outbound data.

There are two basic requirements of honeynet to be perform, both of these principal of successfully protecting a network.

- ***Data capture***: the principal of data capture concerns information gathering. All the information that enters or leaves the honeynet must be collected for analysis. this data must be collected without the knowledge of individuals who are performing malicious activities against the network that is to be protected, collected data is stored different location from the honeynet, it is done so if the hacker compromise the honeynet the data cannot destroyed or altered [10]. So the data is store at safe location where attacker cannot perform their action.

- ***Data control***: the principal of data control concerns protecting other networks from being attacked and compromised by computers on honeynet [10]. If the hacker compromises the honeynet system, then this hacker must be prevented from using this system to attack and compromise production system on other networks. The process of data control must be automated to prevent the attacker from getting suspicious. We do not want the hacker to become aware of fact that system he has to compromise is on honeynet.

- ***Attacker Luring***: Generating interest of attacker to attack the Honeynet. Deployment of honey net should be focused on the threat that an organization is interested in tracking.

III. RELATED WORK

Many of earlier of works in attack or worm detection were network based. Many related work have been purposed on the honeynet. Over the past years, growing number of honeynets have been deployed in the internet.by L. spitzer defines the honeypot, tracking hackers [1]. Their have related work of deployment of low interaction honey pot in an organizational private network have been perposed by the Saurabh Chamotra, j.s. Bhatia in 2011 [3]. The Related work of honeynet is proceed in the the honeynet project know your enemy, proposed by Addison Wesley, 2002 and modified it in 2006. The strategy is to defend one's organization as best as possible, detect any failures in the defense, and then react to those failures. In this primary purpose of honeynet is just gathering the information. Honeynet can use to capture, analyze the botnet that are on their network. In here we desicribe the proposed technique used by John Levine, Richard LaBella use the honeynet to detect exploited systems across large enterprise networks. Here they describe the security mechanism at their connection to network, and improved the security technique when hackers can track the compromise system.in this they implement the proposed technique of honeynet which can easily identify the malicious traffic on their enterprise and easily implemented in earlier years. Under the principal of data capture, all data associated with these exploits is collected for the further analysis. Several researchers have previously studied DDoS attack detection and response, and worm traffic propagation. The Attack detection techniques can be either based on an anomaly detection approach or a static signature-scan technique. A large number of anomaly-detection tools have been designed and implemented previously. In this paper our method of honeynet is based on the use of traffic analysis for attack detection and mitigation techniques, where we have analysis different traffic analysis techniques to detect the attack. In many large enterprise network faced many difficulties to identifying a traffic in the network due to their high bandwidth usages on their networkmake it very difficult to identify malicious traffic on the enterprise network, so we can propose that honeynet can be used to assist the system administrator in identifying malicious traffic on the enterprise network [9].

Traffic from any enterprise network to a machine on honeynet may indicate to compromise system. Our results indicate that analysts can rapidly examine network traffic and detect anomalies far more quickly than with manual tools. Rapidly detecting and classifying malicious activity contained within network traffic is a challenging problem exacerbated by large datasets and functionally limited manual analysis tools.

Even on a small network, manual analysis of network traffic is inefficient and extremely time consuming. Current machine processing techniques, while fast, suffer from an unacceptable percentage of false positives and false negatives. To complement both manual and automated analysis of network traffic, we implemented a honeynet technique by use of the low Interaction honeypot for providing a Simulation of large network topologies.

- Configurable network characteristics like latency, loss and bandwidth
- Supports multiple entry routers to serve multiple networks
- Integrate physical machines into the network topology
- Asymmetric routing
- GRE tunneling for setting up distributed networks

One useful feature of low interaction honeypot like honeyd is its ability to simulate an entire network topology within one machine – with multiple hops, packet losses and latency. This lets us simulate complex networks in test labs; it could also present a make-believe network to an attacker who gets snared in a honeynet. In this data is divided on the basis on known and unknown attack. Known attacks are sending to high interaction honeypot and unknown attacks are sending to low interaction honeypot. As a low-interactive honeypot, it collects information regarding known or unknown network-based attacks and uses plug-in for automated analysis.

IV. HONEYNET ARCHITECTURE

Honeynet technique is used to attack detection for capturing the various traffic on the network.Honeynet can increases both the volume of data that can be gathered, as well as the potential for more complex attacks to be captured. This is allowing to collect all honeynet traffic to analysis the attacks. It can be characterize the traffic for detection of attack and minimal risks and record the all activities or tools of intruders that are going on the system.

In below diagram we explain the various activities of intruder captured by the honeynet. Data is arrival from the internet at through router it can capture the network traffic at the gateway. Gateway that can join the together two network that use different protocol and that serves as an entrance to another network. It can be routes the traffic from workstation to outside the network that is serving the web pages. In the enterprises, the gateway node often act as proxy server and firewall .it can also be associated with both a router, which use headers and forwarding tables to determine where packet are send, and switch provide actual path for packet in and out of gateway. Data are transferred through router that can easily provides the roué to a network traffic, then captured the data in gateway where the honeynet can perform their action such as data captured and data control, where the all data is captured by honeynet in depth. Then these data is protected or under the control requirement our network's activities is Controlled by honeynet or analysis the network traffic.

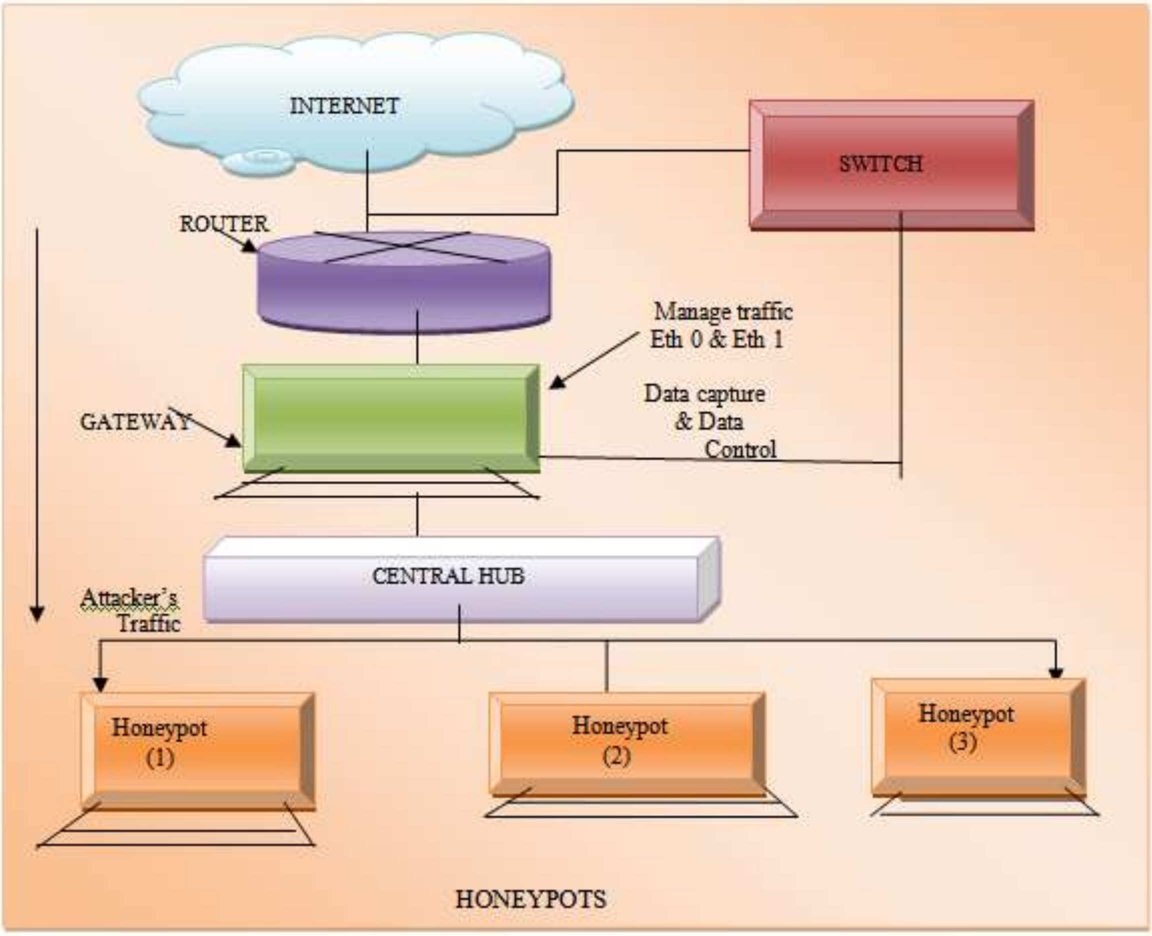

FIG1. Architecture of Honeynet

In the portion of gateway their most important activitity is performed where we collect or captured the attacker's traffic and another activity it can protect our network from hacker then data is transferred to the central hub where all data is controlled and hub can transfer these data to each honeypots. Each traffic or data that is captured by the honeynet can be stored to a different location from the honeynet where the attacker can cannot perform their action. When suddenly attacker can compromise the honeynet then our captured information safe from the any type of hackers activity [10].

In large enterprise network their have some difficulty with the network to determine the malicious attackers or network traffic on the network due to high bandwidth and capacity storage then honeynet technique can the control the bandwidth and data strorage capacity and through this we can easily identify network traffic for large enterprise network.

V. TRAFFIC CHARACTERIZATION

In honeynet we propose a traffic characterization technique for attack detection. Here we describe the honeynet in briefly to capture the malicious traffic of network against the intruders. Honeynet can reduce the false positive and false negative attacks from our network. High bandwidth malicious traffic can not be captured by the honeynet for large network. So it can control the the bandwidth or storage capcity for network traffic so we can easily identify the network traffic, characterize these data in the enterprise network [9].

So traffic analysis is best approach in honeynet to finding the network traffic in different location of our network.through this we can easily detect the attackor mitigate the risk from network. In The network forensic is defined as the activity of capturing, recording and analysis of network data in order to identify the patterns of attacks in that network data [11]. The domain of network forensic is very vast which include capturing of network data, logging, identification of attack in those collected data. In Network forensics involves monitoring network traffic and determining if there is an anomaly in the traffic and whether it indicates an attack. If it is so then the nature of the attack is also determined. Network traffic is captured, preserved, analyzed and an incident response is invoked immediately [15]. Protective measures can be taken on the basis of this information gathered by research honeynet. Ways and means used by attackers can be know and gathered by the research honeypot during an attack. Determination of actions, intentions and even knowing the attackers is possible with the help of information provided by research honeypot. This honeypot is very complex to deploy and to maintain. A large amount of data can be gathered by this. But, it is very time consuming for an administrator.

It can support constant monitoring of all the actions of an attacker as well as they can be recorded while they compromise any system. The most unique and advanced feature of research honeypot is its intelligence gathering. Research honeypots can lead to discovery of new worms. Honeypot functions by capturing attacker keystrokes and records all the activity of attack in the form of packet capturing data [2]. Same is the case when any organization is using this honeypot as a production solution; definitely it is detecting the attack, blocking the attacker and perhaps even prosecuting the individuals involved.

Honeynet can be used for by the organization as a research solution, it is more interested in what tools the attackers are using, where they are coming from, and their activities after they have compromised the honeynet. Thus same honeynet allows us to gather same information, only the difference is in its purpose or either production or research solution. To detect the intrusion in the network traffic and to detect any kind of anomalous behavior, it is very important for forensic engineer to analyze the network data. The investigation of the capture data may lead to incident response towards the findings of the anomalies or suspicious behavior of the traffic [12].

Honeynet is a powerful tool to study the behavior of the attackers as there are not pre-defined set of signatures to detect the attacks. It is able to collect the known and unknown kind of attack.

VI. WORM OR UNKNOWN TRAFFIC REDUCTION

With the help of honeynet we can observe worm traffic in network by the control over the bandwidth. It can found the different type of malicious worm traffic which is harmful for our network it can capture this type worm traffic and reduced the risk from network. Honeynet can reduce clutter from log.Data control is the repression of activity within the honeynet. Determination of ways of avoiding destructive and abusing other machines through the honeynet by the attacker can be done with the help of Data Control.

As we require learning from the moves of an attacker, it demands great planning. We also have to restrict the attacker to use our resources like honeynet and bandwidth for attacking, damaging and abusing other hosts on the same or different subnets. Administrators have to take careful measures to study and make a policy for the attacker's freedom against containment. It is implemented in this way for achieving maximum data control and still not discovered or identified as a honeynet by the attacker [19]. The process of security is implemented in layers.

All the logging, monitoring, and capturing of all threats and intruder can be done in the honeynet. Investigation of captured data gives an approach on the tools, method, techniques and aim of technique is reduce the worm attack from system.honeynet is not software, it is an architecture which we can populate it with the live system LAN where we can generate a record file of worm traffic or analysis the malicious traffic in the network. Any traffic that are entering or leaving the honeynet is suspect.

Honeynet traffic characterization is capture the traffic which are obtained from the defected host machine, where the attacker can perform there actions and network operators increasingly based on monitoring to characterizes these traffic and track these threats.

We identify key characterization of traffic that capture basic properties of worm operations and can be observed with in network traffic summaries. Using network traffic collected at edge router of campus network and network traffic generated real worm instances in virtual machine and honeynet running this approach reliably detect infected host with few false positive [18].We propose that a Honeynet can be used to assist the system administrator in identifying malicious traffic on the enterprise network. By its very nature, a Honeynet has no production value and should not be generating or receiving any traffic. Thus, any traffic to or from the Honeynet is suspicious in nature. Traffic from the enterprise network to a machine on the Honeynet may indicate compromised enterprise system.

It can reduce the false positive because any activities with honeynet unauthorized by definition [1], [2], [3]. It is Real services, applications, and Operating system Capture extensive information, but high risk and time intensive to maintain.it can capture new, unknown, or unexpected behavior or traffic.

It is highly flexible – extremely adaptable and can be used in a variety of environments. It Require minimal resources. Honeynet are focused (small data sets) and captured the information in depth.Honeynet help to reduce false positive. Honeynet help to catch unkown attacks (false negative) [4], [6], [7], [8]. It can capture encrypted activity (cf. Sebek).

For detecting a worm activity in local network, we monitor the traffic generated between local network and external internet. From the traffic, we can catch the peculiar traffic pattern that a worm generates during its propagation. In early stage of worm propagation, such patterns are more observed in outbound traffic than inbound. Because the host infected by a worm spreads many connection requests with same port numbers to distinct destination addresses, we can represent these properties as a record having worm's scan activity. With this information, they can respond to worm propagation more effectively. The second demands to distinguish worm activities from normal traffic and reduce false alarms.

When we monitor traffic in local network, there are differences between inbound and outbound traffic information. Our goals are to accurately identify infected hosts in local network and detect worm propagation activity with low false alarms.To validate our technique, we have gathered traffic traces in our campus backbone network and analyzed the traffic containing many worm activities.

VII. NETWORK SECURITY USING HONEYNET

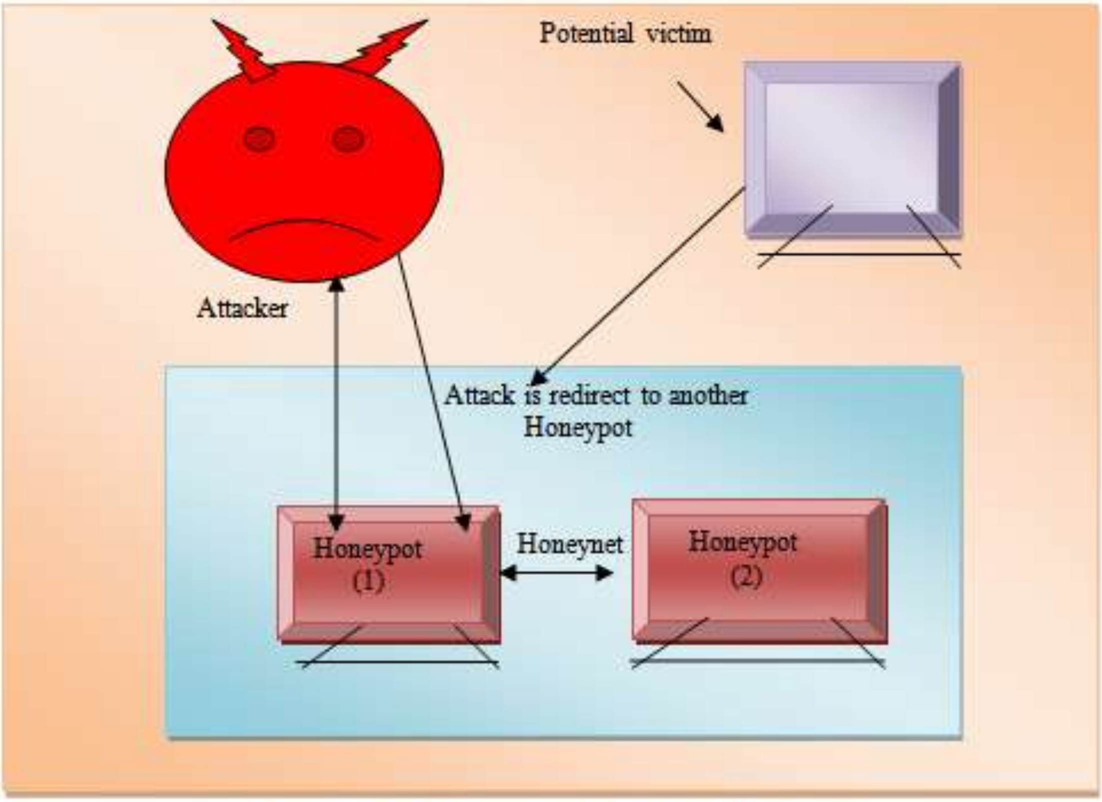

Fig 2) NETWORK Security by the Honeynet

A special kind of high-interaction honeypot is known as Honeynet. The concept of extending a single honeypot to a highly controlled network of honeynet is done by honeynet.

All kind of system and network activity can be monitored and controlled with this kind of highly controlled network architecture. Then, with in this network honeypots are placed. The Honeywall is a transparent gateway behind which honeypots are placed to form a basic honeynet. Honeywall is undetectable by the attackers as it acts as a lucid gateway. It keeps a track of all logging of network activities passing through honeypot [3], [5].

In honeynet diagram we can security mechanism by the use of honeynet which can identify the attacker's activity at our enterprise network. Honeywall is undetectable by attacker it can keep the track logging all the activities which are passed through the network. In this diagram we show the fundamental function of honeynet where it can gather the information about the attacker to provide the security to the compromise system.

In the third diagram which is given below here we record the network traffic that our system requires it for the presence of response activity and monitoring the network traffic. Since there is no application that run and generate the traffic. Then through the honeynet network we can collect behavior profiles, which describe the properties of worm traffic behavior and control the traffic without any knowledge of the attacker [19].

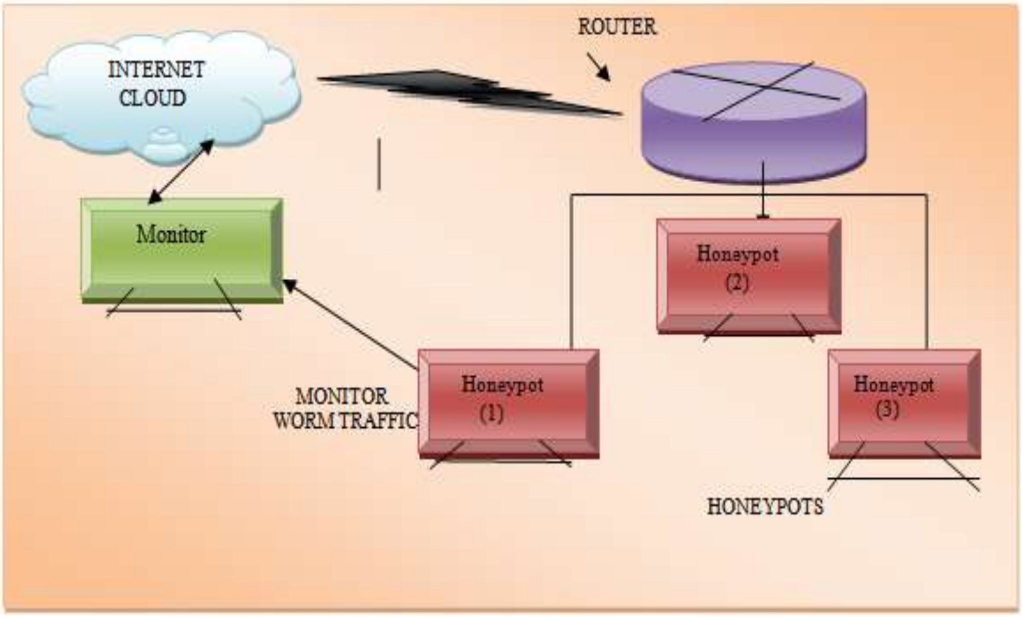

FIG 3) MONITORING NETWORK TRAFFIC BY THE HONEYNET

Our main objective to collect the attack data based on honeynet infrastructure and forensically analyse the collected attack data on honeypot sensors. In this paper we describe attack data after forensic investigation of the network traffic collected on honeypots. Honeynet can increases both the volume of data that can be gathered, as well as the potential for more complex attacks to be captured. Honeywall is act as bridge between the internet and honeynet. This is allowing to collect all honeynet traffic to analysis the attacks. It can be analyze the traffic for detection of attack and minimal risks and record the all activities or tools of intruders that are going on the system.When we are designing our own honeynet that less traffic we create on it then it is easier to analyze our data. and main benefits drawn to this is reduced the clutter in the log. Our main objective objective of honeynet looks like a real, attractive network so that hackers will fully compromise our system not be suspicious that we are monitoring their every move.

VIII. CONCLUSION AND FUTURE WORK

We conclude that honeynet is techinque for detection of attack and minimal the risk from intruders.We can collecting analyzing data for characterize of malicious network traffic in the system.Honeynet is new technology its aim to overcome traditional security tools. Honeynets can early detect new threats and issues. Honeynets are often a research playground to better learn security issues in information systems. Honeynets are a source of in-depth information that classical information security system can't easily provide. Although honeynet obtain lot of focus in recent years and helping to detect attacks and threats efficiently. Tool is easy to deploy and save time. It consists of many tools and functionality which make it powerful to collect extensive information of varieties of threats, so in future scope the implementation of purposed technique is possible. The categorization of these attacks has done with respect to attack type; port etc with statistical graphical distribution. Compared with other security mechanism found that honeypots are easy to use, effective in complex environment, collecting data and information relevant of a good value which can be later analyzed forensically. With the developed solution, the deployment in distributed environment would lead to better and good volume of attack data which are always useful for investigation purpose. Risks are part of Honeynet research and we have to manage it. Honeynets are used to be better prepared to information system attacks. Honeynets can early detect new threats and issues. Honeynets are often a research playground to better learn security issues in information systems. Honeynets are a source of in-depth information that classical information security system can't easily provide.This area is still young and can provide new territories to better secure the information society. In this paper we plan to examine more scanning strategies of worm and improve our technique that can detect unexpected or unknown worms. Furthermore, it is necessary to research the clear differences between traffic patterns of worm and worm-like behavior. And we need to gather and analyse more traffic data for various network conditions.

REFERENCES

[1] L.Spitzer,"honeypots: Tacking Hackers"Adison Wesley, 2003.

[2] C.stoll, "cuckoo's egg: Tracking a Spy through Espionage "The Maze of computer, 1990.

[3] Saurabh, chamotra, j.s Bhatia "deployment of low interaction honeypot in an organizational network"in proceeding in IEEE ETNCC2011.

[4] Christian kreibich, Jon "honeypotcomb creating intrusion detection signatures using honeypot"

[5] Craig Valli, "honeypot technologies and their applicability as an internal countermeasure.

[6] Niels Provos, Thorstenholz,"virtual honeypots: from bonnet tracking to intrusion detection", Addison Welsey Professional.

[7] Vinod Yegneswaran, Chris, Paul Bar fore, "Camouflaging Honeynets" In proceeding of IEEE Global Internet Symposium 2007.

[8] Honeynet.org, "Know Your Enemy: Honeynets," November 2003.

[9] Tobi Wulff and Ray Hunt, "New Approaches to Mitigation of Malicious Traffic in VoIP Networks". November 2010. http://ro.ecu.edu.au/ism/103.

[10] John Levine, Richard LaBella, henry Owen, "the use of honeynet to detect exploited systems across large enterprise networks".proceeding of the IEEE 2003.

[11] Kun-chan LAN, Alefiya Hussain, Debojyoti Dutta "Effect of Malicious Traffic on the Network.

[12] J.S.Bhatia, R.K.Sehgal, Sanjeev Kumar "Honeynet Based Botnet Detection Using Command Signatures". Speinger-verlag berlin Heidelberg 2011.

[13] Ting Fang Yen, "Detecting Stealthy MalwareUsing Behavioral Features in Network Traffic". In august 2011.

[14] Palika Jajoo, Ganesh Singh, Maninder Singh Nehra, "Identification and Forensic Investigation of Network Intruders Based On Honeynet"ISSN: 2248-9622, Vol. 3, Issue 6, Nov-Dec 2013, pp.240-246.

[15] Christian Kreibich, Jon Crowcroft, "Honeycomb. Creating Intrusion Detection Signatures Using Honeypots".in 2003.

[16] N. Provos, .Honeyd - A Virtual Honeypot Daemon, in *10th DFN-CERTWorkshop, Hamburg, Germany*, February 2003.

[17] M. Handley, C. Kreibich, and V. Paxson, .Network Intrusion Detection: Evasion, Traf_c Normalization, end End-to-End Protocol Semantics, In *Proceedings of the 9th USENIX Security Symposium*, 2000.

[18] Soniya Balram and M. Wilscy, "User Traffic Profile for Traffic Reduction and Effective Bot C&C Detection". *Vol.16, No.1, PP.37-43, Jan. 2014.*

[19] NathalieWeiler, "Honeypots for Distributed Denial of Service Attacks"Proceedings of the Eleventh IEEE International Workshops (WETICE'02) 2009.