Special Issue Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, www.ijtrd.com

Honeypot

[1]Pavithra.A and [2]Nithya.V,
[1,2]Department of Computer Science, St.Joseph's College Of Arts And Science For Women, Hosur, TamilNadu, India

Abstract - Internet is growing fast and doubling its number of websites every 53 days and the number of people using the internet is also growing. Hence, global communication is getting more important every day. At the same time, computer crimes are also increasing. Counter measures are developed to detect or prevent attacks, Most of these measures are based on known facts, known attack and network intrusion detection and reaction mechanism. As in the military, it is important to know, who the enemy is, what kind of strategy he uses, what tools he utilizes and what he is aiming for, gathering this kind of information is not easy but important .by knowing attack strategies, counter measure scan be improved and vulnerabilities can be fixed .to gather as much information as possible is one main goal of a honey pot generally such information gathering should be done silently, without alarming an attacker. All the gathered information leads to an advantage on the defending side and can therefore be used on productive systems to prevent attacks. A Honeypot is primarily an instrument for information gathering and learning its primary purpose is not to be an ambush for the black hat community to catch them in action and to press charges against Honeypot are hard to maintain and they need operators with good knowledge about operating systems and network security. In the right hands, a honeypot can be an effective tool for information gathering. In the wrong, unexperienced hands, a honeypot can become another infiltrated machine and an instrument for the black hat community, them. the fous lies on a silent collection of as much information as possible about their attack patterns, used programs, purpose of attack and the black hat community itself all this information is used to learnmore about the black hat proceedings and, as motives well as their technical knowledge and abilities, this is just a primary purpose of a honeypot. there are a lot of other possibilities for a honeypot, divert hackers while conducting an attack are just two possible examples. They are not the perfect solution for solving or preventing computer crimes. This paper will present the basic concept behind honeypots and also the legal aspects of honeypots

Keywords - *Honeycomb, Blackhats, Hybrid Honeypot, VMARE, ID*

I. INTRODUCTION

Due to rapid growth of internet technology, people easily retrieve their information and quickly transfer messages. However, due to such a swift internet growth, if we don't concurrently attach value to basic network by using some malicious code, system vulnerabilities and program weakness. then the attack, devastation and stealing, Tampering of information by the hackers may lead to great permission to make digital or hard copied of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. to copy otherwise, or republish, to post on servers or to redistribute to lists requires prior specific permission and /or a fee Damages and loss of data. Traditionally we use IDS(Intrusion Detection System) and firewall system in network to prevent our damages and to provide network defence against the intruders. But IDS and firewall cannot avail all the information to know the intruders attack and reduce loss caused by attack.

Infected or malicious code according to pei-sheng huang et al "any malicious unauthorized access, the program is not in line with expectations". Such as computer virus, Trojan or backdoor software, worm, dangerous program (risk ware) threads are malicious and malevolent codes properly and knowing the target sites of attack in network, we can provide support to security officials to detect and analyse infected code to guarantee network security. This information is collected by Honeypot and offered to other gears that don't have this information. If we integrate this information together with an IDS and firewall it may lead to reduction of false positive or false negative. We have various complications during the implementation.

Those collected information has some restrictions at various levels and this information are not complete. Now we are presenting various problems statements and flaws which can be used for further research in this area to provide better security. Thus security officials can understand the information and can perform deep analysis to realize the patterns of attacks and risks attached with it.

In 2002, Spitzner defined Honeypot has "A security resource whose value lies in being probed, attacked or compromised. "Further honeypots don't provide any solution to any problem, nor they "fix" anything they are just a tool, it depends upon the user how and in which way they use this tool either for good or for bad.

A honeypot is a computer system which is placed to get compromised to get the information about the blackhats.A honeypot is like any other computer system which contains directories drives in it as real computer system, but its motive is very specific and different. The use of tool system is in this manner is famous among the white and black hats only. One can never eliminate risk, but security helps reduce risk to an organization and protect its valuable resource.

The rest of the papers are as follows.

II. TYPES OF HONEYPOT

In 2007, Marty Roesch suggested, there are the two types of honeypots are research and production.Further, according to Mokube I and Adams M.we can group honeypots according to their aim and level of interaction

A) Research Honeypots

As the name suggest, these types of honeypots are solely used in the research areas. The main aim here is to get maximum information about the black hats by giving them full access to penetrate the security system and infiltrate it. By allowing such an access to black hats, it's easy to know about the tools used and other related information about them.

B) Production Honeypots

This type of honeypot is used to protect company from malicious activities done by black hats. thishoneypot is placed

under the placed under the production network to increase the overall security of the company.Spitzner L and Brucesuhneier model helps us to understand the honeypots. They divide the security into groups as:

- Prevention
- Detection
- Response

- *Prevention* - In this type, as company's point of view they are solely concerned about their security and not much interested to know about black hats. So, they put firewall, usestrong passwords, even try encryption techniques, digitalsignatures, digital certification and provide well know security services. They do these just to keep away black hats from their valuable resources.

- *Detection* - Considering that the prevention doesn't work well, the other solution to overflow attacks is Intrusion Detection System. This technology will help us know whether the system has been compromised or not but, it will not prevent hacker from attacking the system.

- *Response* - We are unable to prevent the black hats to infiltrate our system by the above two approaches. As our system has been compromised, in order to take down the attackers we have to backtrack them by the use of log files. Every system makes a log file, keeps information about everything happening in the system in it. by studying and analysing the log file we are able to find information aboutblack hats, the IP address they used, their network address from which they accessed and the available ports from which they accessed our system. this technique is known as forensic investigation. Based upon the level of interaction that we provide to the black hats to access our systems, we can categorize honeypots as:

- Low Interaction honeypots
- High Interaction honeypots

- *Low Interaction Honeypots*

In the low interaction honeypot, the interaction of the black hats with the system is limited and is for small amount of time thus the black hatscannot intrude the system. this type of honeypot is made keeping in my mind that we are securing ourselves from the intruders. but we get very little information about black hats. so, this approach is widely used in companies where they are concerned about protecting their system from the outer world.

- *High Interaction Honeypot*

In high interaction honeypot, the main emphasis is to get the maximum information about the black hats allowing them to access the whole system or ever tamper it . this is solely research oriented, for those who want to discover new techniques used by the black hats.

III. ADVANTAGES

- Honey pots are placed just to get information about the attacks as they are been recorded in the log files.
- People who target the honeypot are the black hats as they only know about it not the common people.
- Honeypots are not bulky as they are placed just to capture a specific pattern of data i.e. Malicious traffic.
- Honeypots provide us the information about the newly generated attacks, newly defined technologies.

Honeypots are simple and easy to configure. They do not have complex algorithms.

IV. VIRTUAL HONEYNET IN TEACHING AND RESEARCH

- Another
- As honeypots captures the malicious traffic, they also capture the new tools used by the black hats.
- Honeypot detects few false positive and false negative data also.

A honeypot can be placed in a network, with firewall, before firewall and after firewall. We are considering these places because these are the most frequent places from where the black hats accesses the system and we can trap them to get maximum information about them. Our aim is to get maximum information about them by compromising our research data ,so that they may not infiltrate the data again in the future . we are here to know the tools used by attackers, their technologies so that we can update our network security against these tools.

V. APPLICATIONS AND DEVELOPMENT OF HONEYPOT

This section discusses the application domains of honeypot. here we discuss its application in educational areas, internet, with IDS and its implementation.

VI. HONEYPOTS IN EDUCATIONAL RESOURCE

A lab has been established at brigham young university for network security purpose for undergraduate and graduate students called ITSecLab. They use this lab for tracing the malicious traffic in the network. This lab was designed solely for the purpose of experiments on network security by students. In addition to this lab they have implemented a honeypot in their lab to get in touch with black hats and explore its user as an educational tool. the lab is designed as an isolated" Sandbox"in order to keep away the malicious activities from lab. The honeypot is implemented at brigham young university keeping in mind the certain benefits such as it notifies about the new threats, securing the lab at higher level, learning the network and security basics and closely identifies the flaws. One more aspect comes into play when implementation the honeypot, the legal issues that are most important part in implementation Because if the honeypot gets compromised way of implementing the honeypot in educational areas can be done by implementing real or virtual honeynet for better understanding the flaws in network security.Depending upon the use and its advantages, real or virtual or both can be used in educational institution. research on honeynet in a brigham young university IT security curriculum states the advantages of implementing the real and virtual honeynets. In order to predict which scheme is better either the real honeynet or the virtual honeynet, comparisons have been done taking under consideration setup, development, maintenance, data collection, and data analysis defined and considered. in the real honeynets, all the connections have to be considered very generously in order to remove any possibility of fault. if any connection is made wrong, then the whole system gets thrashed. whereas in the case of virtual honeynet, it is implements in virtual environments using VMare in which each network is divided into subnets. It should be considered properly that different ports must be assigned to virtual networks.

VII. HONEYPOT WITH IDS

An intrusion Detection System(IDS) discriminates between the traffic coming from various clients and from the attackers in an effort to simultaneously ease the problem of throughput, latency and security of the network. after that we can present the results of a sequence of load and their response time in the terms of performance and scalability tests, and suggest various types of potential uses for such a system.

In IDS we may use two common type detection level known as Misuse detection and Anomaly detection . in misuse detection the IDS analyses all the various kinds of information that have collected and match it to large database of attack signatures. In abnormaldetection,the administration makes a baseline, or we may say a normal network traffic load, collapse, protocol and packet size. It monitors network and compares it to those baselines.

IDS can be further categories into Network based and host based. in network based IDS all the activities of the host are monitored. honeypots can either be host and/or network based, but generally they are not network based as all interface operation are typing performed over a network connection. Its key utility is that it simplifies the Intrusion Detection Problem of separating "anomalous" from" normal". Thus". thus, any activity on a honeypot can be immediately defined as abnormal.

VIII. HONEYPOT IN INTERNET

The honeypot project measures the actual computer attacks on the internet. According to their most recent results, a random computer is scanned dozens of time a day. A honeypot is a program that takes the form of attractive services, an entire OS, or even an entire network, but is in actual a tightly scaled compartment built to attract an attacker, effectively shunting an intruder safely from production systems for convert analysis. Here honeypot monitors each logs files and every action of an attackers.

If any kind of attack comes, a honeypot provides two things: first the information needed about an attack to develop quick and suitable response in real time and second is the time required to implement that response. during analysis of an attack after it has occurred a honeypot can be used in analysing an attacker's activity (basic information) to develop long term strategic line of action, including tagging which counter measures/patches should be implemented. for other response operations, honeypots can be useful for detecting inside misuse where it is known exactly what to do to attract the "attackers".

Honeypots can be implemented to show its effectiveness by means of three different ways: to deceive, tointimidate, or to provide reconnaissance. To deceive, a honeypot should provide various reasonable responses such that intruder does not suspect it is a trap .to intimidate a honeypot increases the intruder level of risk trough advertisement in unauthorized deception port. for reconnaissance, a honeypot allow vital attack signature information to other security tools such as IDS and firewalls to decrease the number of false alarms.

These are various societal issues attached with honeypot, such as the issue of entrapments, if an attacker is intentionally lured to a honeypot, there must be no implicit permission to access the system. viewing files and not protected since there is no legitimate account or privacy in storing files on a stolen computer or files on a compromised computer without owner's authorization, there islittle or no case law on interception of communication relayed through a compromised computer.

IX. NETWORK SECURITY THROUGH "HYBRID HONEYPOT"

A honey is a system that is made and set up in order to be hacked. it can be used in a different scenario as intrusion detection facility, defence or reaction mechanism moreover, it can be deployed in order to consume the resources of the intruders or distract them from the precious targets and slow them down that wastes their time on the honeypot instead of attacking production systems or servers.

Here again we divide the honeypots into two categories according to their level of low level interaction and high level interaction, the level of interaction can be define as the maximum range of attack possibilities that a honeypot allows an intruder to have, in high level interaction honeypot, attacker interact with real operating system, all the services and program and this type of interaction can be used to observe the attackers performance, their tools motivation and explored vulnerabilities.

This type of high level interaction honeypot can be deploying inside a virtual machine using various virtualization software such as VMware, Qemu, Xen.

X. DEVELOPMENT OF INTRUSION DETECTION SIGNATURES USING HONEYCOMB

This phenomenon generally deals with generation of signatures, at present, generating signatures are tiresome work, manual process that needs detailed. knowledge of each software function that is supposed to be detained. simplistic signatures tend to generate large numbers of the same reason the concept of honeycomb a system that generate signature for infected traffic automatically, isused. here pattern detection techniques and packet header are used. here pattern detection techniques and packet header are used for conformance tests on traffic captured by honeypots.

The purpose discussed about the attack signatures is to explain the characteristic elements of attacks.defining these signatures. as a consequence, different system offer signature must be narrow enough to confine precisely the characteristic aspects of exploit it attempts to address, at the same time, it should be flexible enough to capture variation of the attack. failure in one way or the other leads to either large amounts of false positives or false positives or false negatives.

XI. ARCHITECTURE OF HONEYCOMB

Ledge specific to certain application layer protocols. Each received packet honeycomb to begin same succession of activities:

- If there is any existing connection state for the new packet, that state is updated, otherwise new state is created.
- If the packet is outbound, processing stops here.
- Honeycomb performs protocol analysis at the network and transport layer - Honeycomb performs header comparison in order to detect matching IP networks, initial TCP sequence numbers..
- For each stored connection - If the connection has the same destination port, honeycomb attempts pattern detection on the exchanged messages.

If no useful signature was created in the previous step, processing stops.otherwise, the signature is used to augment the signature pool.

CONCLUSION

In this paper, we present the concept of honeypots and its application. we have implemented and developments honeypots in different technical ways in a network, to provide various security aspects. We have also discussed various types of honeypots and its use with different functionality aspects.

References

[1] Aaron lanoy and George W.Romeney, senior Member, IEEE [2006]A Virtual Honey Net as a Teaching Resource.

[2] The Honeynet project, know your Enemy: Honeynets, April 2001.

[3] Honeynet Research Alliance, project Honeynet website. Retrieved May 16th 2003 from the world wide web: http://project.honey.org

[4] Brain Scottberg et-al. internal Honeypot: Protection or entrapment, 2002.

[5] The Honeypot project, know your Enemy: Revealing the security tools, tactic, and motives of black hats community,2002.

[6] Ram Kumar singh & prof.T. Ramanujam. Intrusion detection system using advanced honeypots, 2009

[7] Cliaord Stoll. Stalking the Wily Hacker. Communications of the ACM. Pp 484- 497.1988.

[8] (2005, August). Know your Enemy: Honeywall CDROM Roo 3rd Generation technology, Honeypot

[9] Project & Research Alliance, [online] Available: http://www.honeynet.org,last Modified: 17 august, 2005.

[10] Hybrid honeypot system for Network Security by kyi lin lin Kyaw, 2008.

[11] Honeycomb. Creating Intrusion Detection Using Honeypots Christian Kreibich, Jon Crowcroft.