International Journal of Interdisciplinary Innovative Research & Development (IJIIRD)

ISSN: 2456-236X

Vol. 02 Issue 02 | 2018

Need of Honeypot Security Mechanism

Anurupa B. Chendge[1], Dr. Praveen Gupta[2]

[1]Student, YMT College of Management, Kharghar
[2]Asso. Prof., YMT College of Management, Kharghar

ABSTRACT

Information security is gaining popularity in organizations & stands alone with respect to security leading to exponential interest to complement the existing methods. A honeypot is a security resource whose value lies in being investigated or negotiated. In this paper we give an overview of honeypots and provide a starting point for persons who are interested in this technology.

Honeypots use many purposes for different organizations. Generally, a honeypot is an information system resource whose value lies in unauthorized use of a resource and values is being misused.
The data security for the organization and individuals are being safe to secure.

Network forensics is used to detect attacker's activity and to evaluate their behavior. Data collection is the important task of network forensics and honeypots are used in network forensics to collect useful data. Honeypot is an new technology with vast potential for security communities. This review paper highlights introduction to honeypots, their importance in network security and improvement in honeypot design.

Keywords: ***Honeypots, security, attackers, honeyed.***

1. INTRODUCTION

The Honeypot technology is used to keep safe our system from attackers. It controls the counter attack from mysterious source of system. The process for discovering and maintaining the network or system is to analyze security procedure and policy. To grant the unauthorized content the hacker hack or misuse the data through internet. This detection provides various functions such as integrity of the system and the content of system configuration, abnormal activities analysis on performance and data, analysis of activities' matching is used to know the attacks.

In the era of information and technology network security has become the core issue in every organizational network. Honeypots are integrated in network with a firewall and Intrusion detection systems to provide solid secure platform to any organization. A Firewall provide the filtering and generate logs to further analyze any malicious activity or any violation policy of access control list, firewall rules. Different approaches like a firewall demilitarized zone (DMZ) have been used but they are not effective for today's network security. Intrusion detection systems then introduced to overcome the shortcomings of existing network. Intrusion detection system silently monitor the network's traffic and give the alerts to tell about any kind of intruders based upon the database of signatures of existing intrusions. A number of issues were with IDS too as facing with an increasing number of false.

Honeypots then introduced in the network to utilize the network's unused IPs and the attacker's behavior is analyzed on these honeypots. Honeypots improve IDS too by decreasing the numbers of false positives.

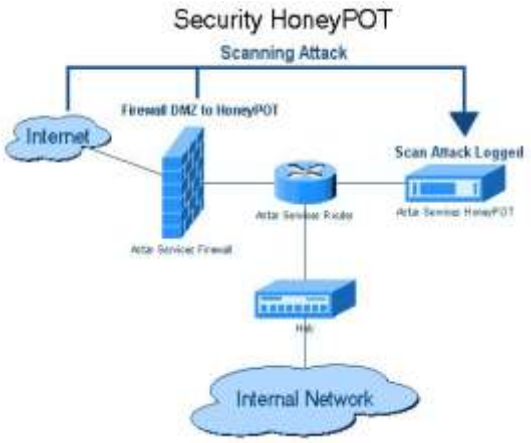

Fig no. 1: Honeypot Security

2. WORKING OF HONEYPOTS SECURITY MECHANISM

Honeypot deployment can be very complex and extremely time-consuming. Because each honeypot addresses only the relative handful of connections it receives, few, if any, organizations have the time or the resources for large-scale deployment of the product.

One solution being developed is the open-source Honeyed (see Figure 1), which monitors unused IP space, instead of a single IP address. Any traffic or connection attempt made to an unassigned IP address is most likely unauthorized or illicit activity. This exponentially increases a honeypot's ability to detect unauthorized activity.

When someone attempts to communicate with an unused IP, Honeyed--which is installed on a single computer--creates a virtual honeypot that interacts with the attacker. Honeyed also has the capability to detect activity on any TCP/UDP port, even if the connection is encrypted or uses IPv6 to tunnel traffic.

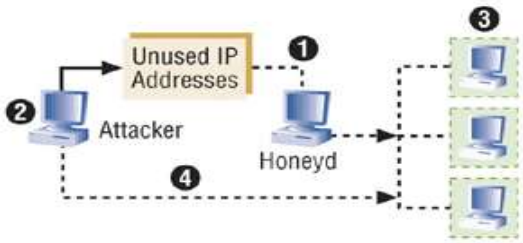

Fig no. 2: How Honeypots Works

3. LEVEL OF INTERACTION OF HONEYPOTS

3.1 Low Interaction Honeypots

On the basis of interaction low interaction honeypots doesn't provide Operating system access to the intruder. It provides only services such as ftp, http, ssh etc. these low interaction honeypots play the role of passive IDS where the network traffic is not modified. Some examples of low interaction honeypots are honeyed, specter, BOF. Honeyed is an opensource tool and the facility of service emulation on honeyed is unrestricted whereas specter is not an open source tool and developed by Neste. The well-known example of low interaction honeypot is Honeyed. Honeyed is a daemon and it is used to simulate large network on a single host. It provides a framework to create several virtual hosts using unused IP addresses of the network with help of ARP daemon for instance, several virtual number of operating systems, server, switches, routers, can be configured on a single host. Furthermore, emulated services include FTP service listening on port 21 (Telnet), login to FTP server etc. Other low interaction honeypot is specter and kFsensor. Specter can monitor total of 14

Tcp ports. Out of these fourteen ports seven ports are called traps and seven are called services. Traps act as a listener of ports i.e. when attacker makes connection with these ports the attempt is terminated and then logged. Services are more advanced wherever there is interaction between attacker and emulating services.

3.2 Medium Interaction Honeypots

Like low interaction honeypots these also do not provide OS access to attacker but chances to be probed are more than low interaction honeypots. Some examples of medium interaction honeypots are Nepenthes, Dionaea, honeytrap, mwcollect. These honeypots also provide faked services to the attackers. Mwcollect and nepenthes can be used to collect the spreading malwares.

3.3 High Interaction Honeypots

These are the most sophisticated honeypots. These are difficult to design and implementation. These honeypots are very time consuming to develop and have highest risks involved with this as they involve actual OS with them. In high Interaction Honeypots nothing is simulated or restricted. Some example of High interaction honeypots isSebeka, Argos. As these honeypots involves real operating system the level of risk is increased by many extents, but to capture large amount of information by allowing an attacker to interact with the real operating system, it is a kind of trade off. This helps in capturing and logging of attacker's behavior that can be analyzed in later stage.

4. PURPOSE OF HONEYPOTS

4.1 Research Honeypots

Research honeypots are basically used to attain information about the new ways of attacks, new attacks, viruses, worms which are not detected by IDS. These honeypots are used for research purpose. Mostly educational entities, military or government organizations, these kinds of honeypots are used to gather information about motives and new tactics about the black hat community. These honeypots never add direct value to the organization, difficult to maintain and deploy, complex in architecture, but provide extensive information which is worth to develop new policies to protect the organizational network. Research Honeypots are used to gain Information about black hat community Research honeypots are used. Its primary function is to follow the footprints of attacker and gain knowledge about the new ways of attacks performed threats.

4.2 Production Honeypots

Production honeypots are easy to deploy, use and capture less information and are primarily used by companies or corporations. These honeypots are placed along with the production server inside the production network of the organization to improve overall security. A production honeypot is one which is used within organization to prevent attacks and mitigate risks. It provides immediate security to production resources. Production honeypot tend to duplicate the production network or provide some services such as Ftp, Http, SMTP to the attackers. Commercial organizations get more benefits from production honeypots. It addresses some challenges to IDS because of its simplicity. Sometimes attack is too recent to the vendors in such situations IDS doesn't give any alert as it uses it is limited to the signature-based database for detection of intruders. Sometimes untuned IDS alarms too much on normal network traffic. This is called false positive. Honeypots address these challenges as all the traffic sent to honeypots is unauthorized that means there is no false positives no false negatives and large data sets to analyze.

5. IMPORTANCE OF HONEYPOT

The use of honeypots and honey nets improves network security and its systems. Honeypot will be useful in these three areas.

A honeypot will not stop an aggressor from enter into a network. But, on the other hand, all traffic originated by the intruder is registered and can be analyzed, therefore it is possible to get information that will allow, in another

Occasion, the prevention of the same attack. That is, honeypot does not stop attacks against the network or against one determined ports (firewall) of a system. That's why it is not like an Intrusion Detection System (IDS). However, as it is simpler to invade, it can make the aggressors invest its efforts in attacking it, instead of trying to penetrate inside strategical servers. As for the detection, the profits are more considerable. The reason of this is simple: if the complementary tools, such as networks IDS, were flooded with great flows of traffic, they will have difficulties in processing them. Separating the useful traffic out from the malicious traffic is sometimes very complicate. One of the strategies of crackers consists of Occupying a IDS, in order to generate a great number of alarms. These false positives (false alarms) and the filtering of the useful data continue to be issues where the IDS need to be Improved. A honeypot does not have this problem, because all traffic originated or destined to the emulated hosts by default Suspected /hostile. There should not be traffic for such systems because they are not announced or registered in DNS. Although this does not mean that the false positives are impossible, the possibility to happen is far less of that using a Network IDS.

6. IMPROVING HONEYPOT DESIGN

Earlier honeypot systems were based on the idea of placing a small number of attractive targets in locations where they are likely to be found and would draw attacker's attention towards them. However, this defense mechanism offered a little as it only consumed a small portion of the overall intelligence space and has little effect on change the characteristics of the typical intelligence probe. The original Deception Tool Kit (DTK) by Cohen provided the low probability of detecting the deception and the extreme localization of deception under previous honey pot systems. Under DTK, deceptions are spread among the normal systems in a network in such a way that unused services on those systems are consumed with deceptions. This leads to two effects: 1. it spreads the deceptions over a large portion of the IP/port address space 2. It increases the percentage of deceptions in the environment, thus increasing the likelihood of an intelligence probe encountering a deception rather than vulnerability.

7. CONCLUSION AND FUTURE SCOPE

Honeypots mechanism is used for security purpose. Honeypots allows to interact with attackers for particular activity. Honeypots is used for security purpose by preventing, detecting and responding to attacks. Honeypots try to defend against threats.

Honeypots have tremendous potential for the security community, and they can accomplish goals few other technologies can. Like any new technology, they have some challenges to overcome. Most likely none of these problems will ever be completely solved or eliminated.

18 are a variety of honeypot options, each having different value to organizations. We have discussed the value of the honeypot and how they reduce the attacks. We have categorized two types of honeypots, production and research. Production honeypots help reduce risk in organization. While they do little for prevention, they can greatly contribute to detection or reaction. Research honeypots a different in that they are not used to protect a specific organization. Instead they are used as a research tool to study and identify the threats in the Internet community. Regardless of what type of honeypot we use, keep in mind the 'level of interaction'. This means that the more the honeypot can do and the more we can learn from it, the more risk that potentially exists. We will have to determine what is the best relationship of risk to capabilities that exist for us. Honeypots will not solve in organization’s security problems. Only best practices can do that. However, honeypots may be a tool to help contribute to those best practices. Although Honeypots have legal issues now, they do provide beneficial information regarding the security of a network. We think it is important that new legal policies be formulated to foster and support research in this area. With the different types of honeypots such as BOF, Honeyed, Specter etc. we can solve the current challenges and make it possible to use Honeypots for the benefit of the broader Internet community.

The trend of using honeypot is very traditional in network security. It has become necessity of the security for information to lure attackers to some other fake sites in the network than the actual site, where real resources of information are available. Even these honeypots could be extended to honeynets, where attacker

deals with the bunch of honeypots. The log files analyzed through these honeypots and honeynets could be used to enhance the Intrusion detection system to make it smarter in catching intrusions.

8. REFERENCES

[1] Spitzner, L. Open Source Honeypots: Learning with honeyed, Security Focus, 2003.
[2] Wikipedia, http://en.wikipedia.org/wiki/Honeypot(computing)
[3] Martin, W.W. Honey pots and Honey nets –Security through Deception. http://www.sans.org/reading_room /whitepapers/attacking/41.php, SANS Institute, 2001, As Part of the Information Security Reading Room. [7] John Carroll, Computer Security, 3rd ed., Butter worth Heinemann, 1997.
[4]https://pdfs.semanticscholar.org/ac06/b09e232fe9fd8c3fabef71e1fd7f6f752a7b.pdf
[5]http://searchsecurity.techtarget.com/feature/Honeypot-technology-How-honeypots-work-in-the-enterprise
[6]http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.63.5385&rep=rep1&type=pdf
[7]https://www.researchgate.net/publication/228933207_Honeypots_as_a_security_mechanism