ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

Overview of Honeypot Technology

[1] Yarlagadda Durga, [2] Priya Solanki, [3] Sai Krishnam Raju G
[1][2][3] 6th sem, Department of CSE,RYMEC,Ballari,Karnataka.

Abstract: **- Honeypot is a computer security system that includes files, directories in it just like a real computer. The target of honeypot is to attract hackers to fall into it to watch their activities. It is a fake system that looks like a real system. They differ from other security systems since the aim of honeypot is not to find one solution to a particular problem, instead they are applicable for various security problems and finding several approaches for them.**

***Keywords*— Honeypot, Network, Security, Attackers**

I. INTRODUCTION

In computer technology, honeypot is a decoy system, which consists of a computer, data or a network site that appears to be part of a network but actually it is deployed to track hackers with his activities [5]. The main aim of honeypot is to divert malicious traffic away from super system. If a system is about to face a critical attack an alert message is provided by the honeypot. It gathers information about the attackers and their methods. According to Lance Spitzner[1],"A honeypot is an information system resource whose values lie in unauthorized or illicit use of that resource". The honeypot security mechanism does not replace any of the traditional security mechanisms, but add another layer of security. It will not prevent attacks, but its job is to divert attacks from real system and gather information about that attacks.

1.1 The Basic Architecture of honeypot

The honeypot works over internet as they attack the attackers over a network. From fig1.1, it is clear that a separate network is created in a demilitarized zone (DMZ). A service router is used to separate two networks called WAN (internet) and LAN (internal network). The router is configured in such a way that it points to a DMZ machine which acts as the honeypot for any new incoming connections that are not defined in the routing table or firewall rules. If a DMZ was not defined in the router then the incoming connections would be discarded [12].

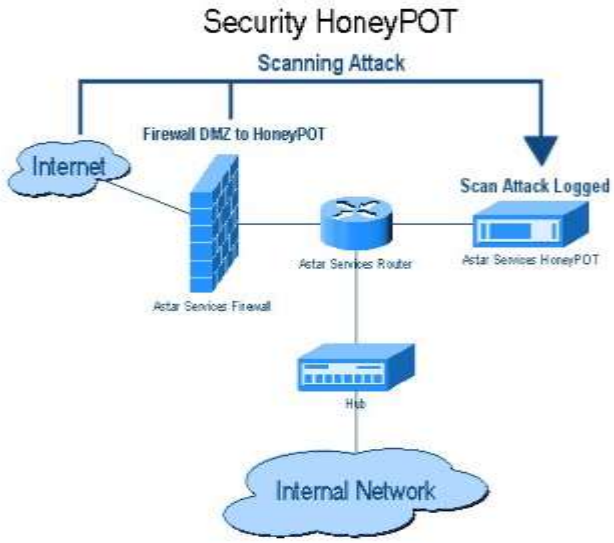

Fig1.1: Basic Architecture of honeypot

The main difference between the firewall and honeypot is a honeypot allows all incoming traffic to come in but stop them to move out whereas firewall stops an unauthorized activity to enter into a system.

II. LITRATURE SURVEY

Clifford Stoll and Bill Cheswick [2] published the first studies of honeypot in 'The Cuckoo's Egg' and 'An Evening with Berferd' respectively in the year 1990-1991. Fred Cohen [3] introduced the deception toolkit version 0.1 which gave an idea of first honeypot structure. CyberCop Sting was the first commercial honeypot released in the year 1998 along with which a BackOfficers friendly honeypot was also introduced that was free and easy to configure. It is working under the windows operating system.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

Most of the people tried this software and the concept of honeypot became more and more known among people. In 2001, Honeypot started to be used for capturing malicious software from internet and being aware of new threats. Companies began to use honeypots in their systems to improve security and see the malicious traffic. Finally in the year 2002 honeypots became popular and improved in their functionalities, so became interesting for researches and companies.

III. PROPOSED SYSTEM

Honeypot is classified on the bases of its use, as follows:

3.1 Types of honeypots [13]:

a. Production honeypot:

Production honeypot is used to protect the company from attacks. As shown in fig3.1, honeypot are placed inside the production network with other production servers by an organization to improve their overall state of security. They capture limited amount of data. Production honeypot follow into the level of low-interaction because the security administrator watches the hacker's movements carefully and tries to lower the risks that may come from it towards the company. They can be deployed easily. They give less information about the attackers than research honeypot.

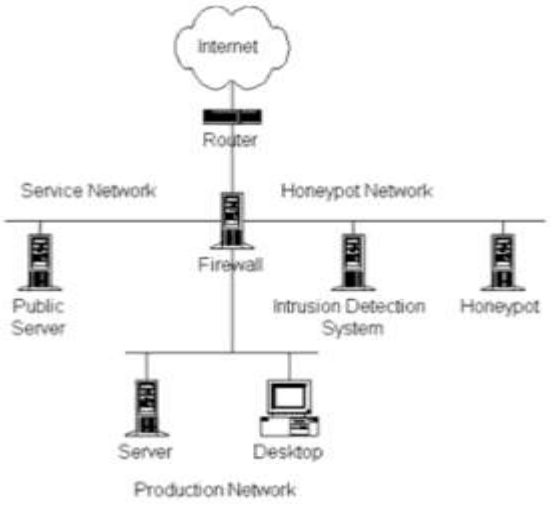

Fig3.1: Production Honeypot

b. Research honeypot:

This type of honeypot is mostly used by military, research and government organizations. They capture huge amount of data. Their aim is to discover new threats andlearn more about the blackhat attackers and his community. Blackhat attackers are those who are skilled hackers and they utilize their ability in illegal works. The objective is to learn how to protect the system better; they do not bring any direct value to the security of an organization. Research honeypot are complex to deploy and maintain.

3.2 Levels of interaction:

The levels of interaction in honeypot are categorized into three levels as mentioned below:

a. Low level interaction

In low interaction honeypot, the amount of data collected is less compared to other honeypot systems. From fig3.2, there is no functioning of the operating system in this level of interaction. They are limited, so the risk that was taken from intruder is not big either proportionally. They can be used to identify new worms or viruses and analyzing the traffic that is going on through network. They are easy to configure and understand. Honeydis one of the most commonly used low level interaction honeypot. Its last version (1.5c) has been released on 2007.

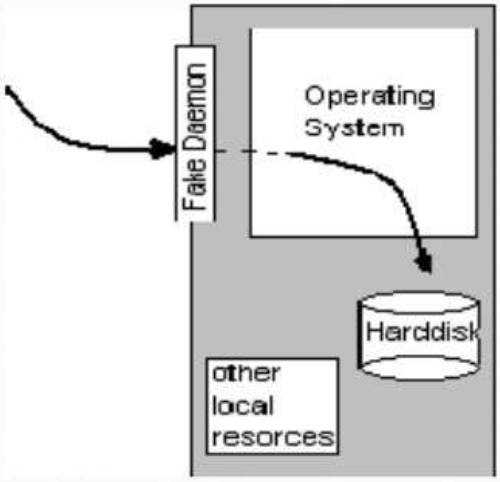

Fig3.2: Low level interaction

b. Medium level interaction

Medium interaction honeypot are more advanced than low interaction honeypots. There is no existence of operating system. They provide more information and more complicatedattacks from the hackers.As it is more advanced, it has more security holesso that hacker can access the system. Mwcollect, honeytrap and Nepenthes are some of themedium interaction honeypots that are used today.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

c. High level interaction

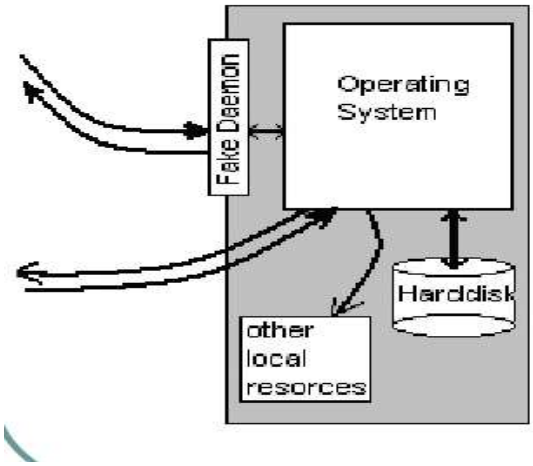

Fig 3.3: High level interaction

High interaction honeypot are the most advanced honeypot. Unlike low interaction and medium interaction honeypot, there is an operating system, now the hackers can perform anything in it. Proportionally, more data can be captured from the hackers activities. When the matter of security comes, it is the most risky because it provides access to hackers without any restrictions. This kind of honeypot are very time consuming and difficult to maintain. Honeywall is a good example of high level interaction honeypot.

3.3 APPLICATIONS OF HONEYPOT[8]

In present time honeypot are widely used in different fields and this paper discusses some of the fields where honeypot has their demands.

a. Unsafe Environment

Honeypot is a sensitive device i.e. it has to be installed in a safe environment because in case of unsafe environment the IP address and port number of honeywall can be accessed easily. Honeypot provides an adequate step for improving efficiency rate of system relates to their security.

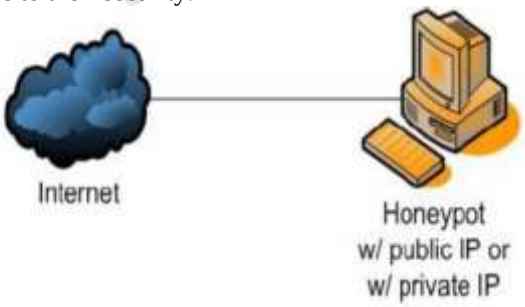

Fig3.3: Unsafe Environment

b. Protected Environment

In protected environment, as the name implies a firewall is added to the honeypot which limits the access to honeypot system. This firewall helps in protecting the honeypot system related to IP address and Port Number as IP address and Port number can't be accessible to every client. This concept does not affect the continuity but add some limitations.

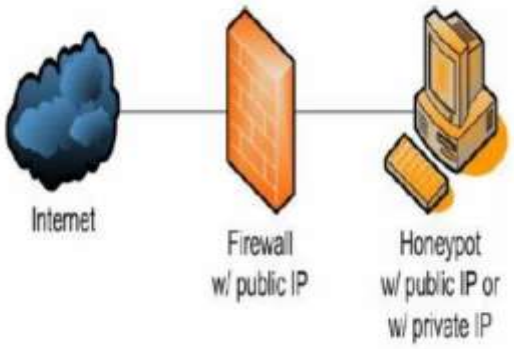

Fig3.4: Protected Environment

c. Network Security

To increase your network securities deploy a honeypot system on your network that acts as a decoy and lures potential hackers like bear's get lured to honey [4]. By following all the activities of honeypot one can easily find out the viruses and worms in the system.

3.4 ADVANTAGES[6]

1. Honeypot provides a good platform for those who deal with security in order of learning.

2. Honeypot have a simple design and are easily implemented that makes it a more favorable to be used in organizations. Honeypot can capture attacks and give information about the attack type.

3. Honeypot are not bulky in terms of capturing data because they only deal with the incoming malicious traffic not the entire traffic.

4. Many security problems in the software sectors are solved by using honeypot.
5. Using honeypot we can easily capture the information about the attackers, which will help the security administrators.
6. Installation of honeypot is very easy, no complicated steps are involved.
7. Once the honeypot is installed to a system there is no need of software programs updated, installed, or modified.

8. They notice the new attacks and further gain knowledge of how to defend a system against these attacks.

3.5 DISADVANTAGES [9]

1. We can capture data into a honeypot only when the attacker is attacking the system actively. If the attacker does not attack the system, it is not possible to capture information.

2. If there is an attack occurring in another system, our honeypot will not be able to identify it. So, attacks not towards our honeypot system may damage other systems and cause big problems.

3. If the system is accessible using a fingerprint this may turn as a drawback if the hacker is intelligent and try to access the system by using fingerprint then he will be able to distinguish between the real system and honeypot system easily.

4. If the attacker is well intelligent and knows the concept of honeypot, he could then try to attack the honeypot system itself that leads to a big trouble for the entire organization.

IV. **CONCLUSION**[10]

Honeypot is a blooming technology in the field of computer security system. Honeypot is computer security software which is virtually installed in a computer system to increase your network securities. It acts as a decoy and lures potential hackers like bear's get lured to honey. Honeypot increases the security of an organization by providing less cost-effective solutions. They are not only applicable to large scale organizations but also to a single computer system as it provide some additional security. Honeypot demonstrated their value as a research tool in the field of Information Security. It is a powerful educational tool in the modern classroom. Honeypot gives enormous potential for the information technology community. Honeypot not only collects the information about the firewall hackers but also the hackers who works for the own company[7]. In Honeypot, there is not only a single tool to solve a specific problem even they have high flexible technology with variety of different roles to be performed. It is different from all traditional, since there is an extra protection layer added in honeypot security mechanism.

REFERENCES

[1] Lance Spitzner: https://www.linkedin.com/in/lance-spitzner-0ab0ba1

[2] Clifford Stoll and Bill Cheswick: https://www.foo.be/cours/dess-20102011/honeypot-introduction/honeynet-intro.pdf

[3] Fred Cohen: https://www.symantec.com/connect/articles/value-honeypots-part-two-honeypot-solutions-and-legal-issues

[4] https://krazytech.com/

[5]https://en.wikipedia.org/wiki/Honeypot_(computiing).

[6]https://infosecaddicts.com/advantages-vsdisadvantages-of-honeypots/

[7]http://www.divaportal.org/smash/get/diva2:327476/fulltext01

[8]Snehil, Atul Tyagi, Rishi Kumar1, 2M.tech (CS & E), 3Assistant Professor (CS & E), Amity University,Noida: http://www.iraj.in/journal/journal_file/journal_pdf/3-174-143867333032-40.pdf

[9] www.iformit.com

[10] https://hstreasures.com/honeypots-42433/

[11] https://blog.rapid7.com/2016/12/06/introduction-to-honeypots/

[12] https://link.springer.com/chapter/10.1007/3-540-27301-8_20

[13] https://www.ijedr.org/papers/IJEDR1504100.pdf