International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 08 | Aug-2017 www.irjet.net p-ISSN: 2395-0072

HONEYPOT- AN OVERVIEW

Arockia Panimalar.S [1], Balaji.K[2], Vignesh.S.R[3], Karthik.E[4]

[1] *Assistant Professor, Department of BCA & M.Sc SS, Sri Krishna Arts and Science College, Coimbatore, India*
[2,3,4] *III BCA, Department of BCA & M.Sc SS, Sri Krishna Arts and Science College, Coimbatore, India*

Abstract - *Now a days, people are using internet all over the world regularly. It is being a part of our daily routine. Attack on the internet also keeps on increasing and it cause harm to our security system. So, it is necessary to have a security system that has the ability to detect the attacks and block them. "Honeypot is the proactive defense technology, in which resources placed in a network with the aim to observe and capture new attacks".*

Key Words: **Honeypot, Network Security, Honeynet, Intrusion-detection, Hacking**.

1. INTRODUCTION

Honeypot is term that belongs to the computer system. It's a trap set in order to detect, reflect or somewhere take some counter measures to any unauthorized activity performed by an authorized or an unauthorized person or a system. Honeypot lures the hacker into the system and monitor the processes that are started and running on the system by hacker. In other words, honeypot is a trap machine which looks like a real system in order to attract the attacker. Honeypot follows beware technology. It is a prior way to save data from hackers. Honeypot generates an alarm to the administrator of the system while attacker attacks the system and provided a wakeup call to the client in order to check out the activities of attacker. Honeypot technology is used in network safety defense and different honeypot based distributed intrusion prevention model are developed. Honeypots provide a cost effective solution to increase the security posture of an organization.

2. HONEYPOT BASICS

A. Honeypots

A honeypot is an "Information system resource whose value lies in unauthorized or illicit use of those resources". A honeypot is a computer system. There are files, directories in it just like a real computer. However, the aim of the computer is to attract hackers to fall into it to watch and follow their behaviour. So it can be defined as a fake system which looks like a real system. A server that is configured to detect an intruder by mirroring a real production system. It appears as an ordinary server doing work, but all the data and transactions are remotely being used. Located either in or outside the firewall, the honeypot is used to learn about an intruder's techniques as well as determine vulnerabilities in the real system. Honeypot resource has no real use. In other words, normal users will never connect to it. It is setup only to lure the malicious users to attack it. Since, a honeypot resource has no real use, and thus, if a system administrator notices a user connecting to it, then 99% of the times that user is a malicious one.

B. History of Honeypots

- 1991 – Publications named "The Cuckoos Egg" and "An Evening with Berferd" was published which set as an origin to honeypot.
- 1997 – First type honeypot named Deceptive Toolkit was released.
- 2002 – Got shared all around the world.
- 2005 – The Philippine Honeypot Project.

3. HONEYPOT CLASSIFICATION

A. Based on the Level of Interaction

It's classified into three types based on the level of interaction:
1. Low-interaction honeypot
2. High-interaction honeypot
3. Medium-interaction honeypot

Low-interaction honeypot: This type has limited level of interaction with the external system. There is no operation system for attackers to interact with, but they implement targets to attract or detect attackers by using software to emulate features of a particular operating system and network services on a host operation system. Low-interactive honeypots are a safer and easy way to gather information.
Example -FTP

High interaction honeypot: It has a very high level of interaction with the intrusive system. It gives more sensible experience to the aggressors and accumulates more information about planned assaults; this likewise includes high danger of catching of entire honeypot.
Example – Honeynets- typically used for research purpose.

Medium-interaction honeypots: These honey pots are sophisticated than the lower-interaction honeypots. It is also called as the mixed-interactive honeypots. It furnishes the assailant with a hitter figment of the operation framework so more mind boggling assaults can be logged and broke down.

Example- Honeytrap- it dynamically creates port which allows the handling of some unknown attacks.

Honeypots Interaction			
	Low-INTR	**Medium-INTR**	**High-INTR**
Alerts	Medium	Low	High
Direct Attack	High	Null	Medium
Efficiency	Low	Low	High
Info in-depth	Low	Low	High

B. Based on Purpose

Honeypots can be classified based on the purpose as Research honeypot and Production honeypot.

Research Honeypot: A research honeypot is used to learn about the tactics and techniques of the Black hat community. Research honeypots are used to gather intelligence on the general threats organizations may face, which gives the organization a better protection against those threats. Its fundamental objective is to pick up information about the path in which the assailants advance and performs lines of assaults. They are essentially utilized by associations like colleges, governments, the military and intelligence systems to take in more about threats.

Production Honeypot: The production honeypots are just meant to ensure the system. It is very easy to construct and deploy, as they require less functionalities. They secure the framework by identifying assaults and offering cautions to administrators. It is normally utilized inside an organization domain to secure the organization.

C. Based on Hardware Deployment

Physical Honeypots: It is a single machine running a real OS and real services, where honeypot is connected to a network and is accessible through a single IP address. Physical honeypots are less practical in real scenarios due to their limited view of their single IP address and high cost involved in maintaining a farm of physical honeypots.
Example: Honeynets

Virtual Honeypots: They are usually implemented using a single physical machine that host several virtual honeypots.
Example: AGROS.

4. DESIGN OF HONEYPOT

A. Honeypot System

A simple honeypot system is basically a combination of three different modules i.e. Induced Module, Deceived Module and Analysis Module.

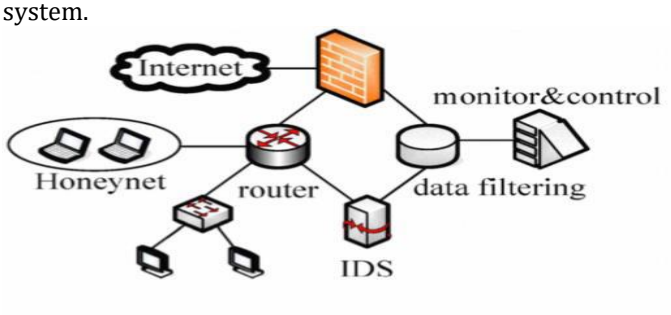
Induced Module: makes the attacker to get attracted towards the honeypot system.

Deceived Module: Simulates fake information from the database which is being handled by the attacker.

Analysis Module: Activities performed by both of these modules are stored and are being analysed by the analysis module.

B. System Architecture

The whole network is firstly protected by a firewall then by a router. The compartmented layers of data are separated from the network inside the organisation and outside operations network. Organization network is then ensured by a component called as honeynet, which is a network of computers cooperation in honeypot architecture. For additional security and detection, IDS is acquainted into the system.



C. Working

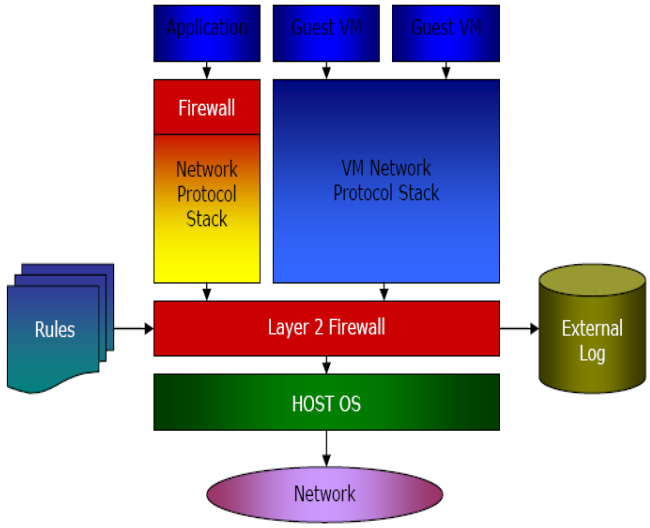
Honeypot is a system to collect intelligence. They are usually placed behind the firewall. Honeypot provides various services and holes which are used to induce various attacks and attack's info. At the point when an interloper tries to enter the framework with a fake personality, the overseer framework will be advised. As indicated by Open Web Application Security Project (OWASP) some best assaults recorded were SQL infusion and XSS. When somebody tries to enter the framework, a log is created about every one of the passages. Despite the fact that the interloper prevails with regards to entering the framework and catches the information from the database, we can trick them by giving fake information, this is finished by honeypot, yet gatecrasher won't know about this fake data. So by this we can spare our framework and trick interlopers.

5. BUILDING A HONEYPOT

To build a honeypot, a set of virtual machines (VMs) are created. They are then setup on a private network with the host OS. To facilitate data control, a state-full firewall such as IPTables can be used to log connections. This firewall would typically be configured in Layer 2 bridging mode, rendering it transparent to the attacker. The final step is data capture, for which tools such as Sebek and Term Log can be used.

Once data has been captured, analysis on the data can be performed using tools such as Honey Inspector, Private Message and Sleuth Kit. This approach is found to be remarkable in its simplicity and feel that a few significant issues need to be brought to light.

1. The choice of a private host-only network. Though this may seem counter intuitive at first, there is a relatively sound reasoning for doing so.
2. While bridging the VMs on to the physical network would seem like a better approach because it transparently forwards packets to the VMs and eliminates an additional layer of routing, it requires an additional data control device which will monitor the packets being sent from the VMs. The operation of data control cannot be performed by the hostOS when the VMs are in bridged mode, since all data from the VMs bypass any firewalls or IDSs which exist at the application layer on the host, as shown in the figure below.
3. The firewall on the host should be transparent to the attacker. This requires considerable effort, since firewalls by default work at Layer 3 or greater. At long last, once a honeypot is traded off, a reclamation instrument must be executed with the goal that it is right away removed the system and every one of its openings precisely stopped before setting it back on the system. This is currently a manual process and can only be partly automated.



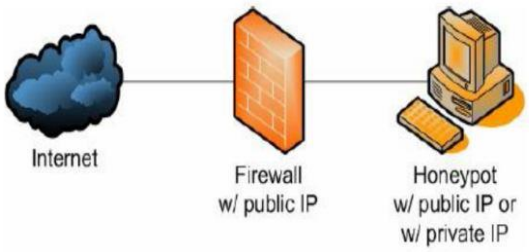
6. APPLICATIONS OF HONEYPOT

A. Unsafe Environment

Honeypot is a sensitive device so that it has to be installed in a very safe environment. Honeypot provides an adequate step for improving efficiency rate of system relates to their security. If the honeypot is not installed in an unsafe environment there are more chances of accessing IP address and port number of honeywall.

B. Protected Environment

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.



7. HONEY POT PRODUCTS

A. Back Officer Friendly (BOF)

BOF is a light weight honeypot and free to distribute. BOF speaks to a precise refining of the thoughts and bits of knowledge of honeypot. BOF user can have clear view of the attacking process. BOF copies a few regular administrations, for example, http, ftp, telnet and mail. BOF logs, alarms and reactions a fake answer at whatever point somebody interfaces with such ports. BOF is created by Marcus Ranum.

B. SPECTER

Specter is a commercial production honeypot whose value lies in detection. It's also an example of Low Involved Honeypot. Spector can simulate 13 different operating systems in application level including Windows, Linux, Aix, Solaris, and MacOS. It is similar to BOF it also emulates services like FTP, Telnet, HTTP etc. Attacker can't utilize the application to interact with the OS.

C. HoneyD

Created by Niels Provos, Honeyd is a powerful production honeypot, which can be used for attacks detection and reaction. It is a Low Involved Honeypot. First, it can emulate over 400 kinds of OS at IP stack level. This hides the guest OS before attacker. Second, emulating hundreds of computers at a single machine by use of Arp spoofing. Third, Honeyd is

Open Source honeypot system. It copies services like FTP, Telnet, and HTTP and copies different operating System.

D. MANTRAP

It is Highly Involved Honeypot. It gives more in-depth knowledge on malicious attackers. It copies Services like FTP, Telnet and HTTP and so forth. It copies diverse Operating Systems also.

8. TRENDS AND ADVANCES

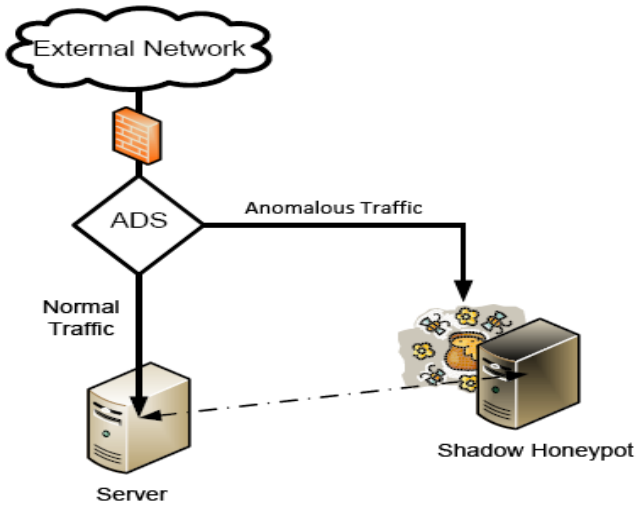
A. Honeynets and Honeyfarms

Honeynets and honeyfarms are the names given to gatherings of honeypots. Honeyfarms have a tendency to be more unified. Gathering honeypots give numerous cooperative energies that assistance to relieve a large number of the insufficiencies of conventional honeypots. For example, honeypots frequently confine outbound movement keeping in mind the end goal to abstain from assaulting non-honeypot hubs. In any case, this confinement enables honeypots to be recognized by an attacker. These redirection hubs likewise carry on like genuine casualties.

A collection of honeypots are combined to create a single honeynet. Honeynet represents the highest level of research honeypot. Honeynets extend to concept of single honeypots to a network of honeypots. Deploying a Honeynet requires at least two devices: a Honeypot and the honeywall. New strategies for data catch and data control proposed by honeynet extend indicate more noteworthy adaptability and higher get to control capacity.

B. Shadow Honeypots

Shadow honeypots are mix of honeypots and peculiarity location frameworks (ADS), which are another contrasting option to administer based interruption recognition frameworks. Shadow honeypots initially section atypical activity from general movement. The abnormal activity is sent to a shadow honeypot which is an occurrence of a honest to goodness benefit. In the event that an assault is distinguished by the shadow honeypot, any adjustments in state in the honeypot are disposed of. If not, the exchange and changes are effectively dealt with. While shadow honeypots require all the more overhead, they are profitable in that they can identify assaults dependent upon the condition of the administration.



9. MERITS AND DEMERITS

A. MERITS

- **Data collection** – It stores only limited data with high value.
- **Simplicity** – Honeypot involves easy implementation and has a simple design.
- **Resources** – Honeypot stores only those data which are coming to them but many other security tools get overloaded in terms of bandwidth.
- Honeypot reduces the chances of false positive and false negative.
- Honeypots provides a good platform for those who deal in security in order of learning.
- They are simple to understand, to configure and to install.
- They do not have complex algorithms. There is no need for updating or changing some things.

B. DEMERITS

- We can only capture data when the hacker is attacking the system actively. If he does not attack the system, it is not possible to catch information.
- 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.
- A Honeypot which is not properly contained will bring risk to rest of the network.

10. CONCLUSION

A honeypot is an instrument. How we utilize that apparatus is dependent upon us. There are an assortment of honeypot alternatives, each having diverse incentive to organizations. It's an innovation which is not only for a major association

but rather this is likewise helpful for a single computer. Generation honeypots help lessen chance in an association. While they do little for anticipation, they can incredibly add to discovery or response. Research honeypots are diverse in that they are not used to secure a particular organization. On the off chance that we discuss the future work in the field of honeypot at that point there is as yet a major degree as honeypot could be utilized as a part of numerous more fundamental models of intrusion detection system and furthermore could be useful in enhancing network security.

11. REFERENCES

[1]Michael Beham, Marius Vlad and Hans P. Reiser, "Intrusion Detection and Honeypots in Nested Virtualization Environments", in 978-1-4799-0181-4/13/$31.00 ©2013 IEEE.

[2] http://www.rbaumann.net

[3] http://www.christianplattner.net

[4] http://www.honeynet.org

[5] http://www.en.wikipedia.org/Honeypot

[6] Mr. Kartik Chawda, Mr Ankit D. Patel, "Dynamic & Hybrid Honeypot Model for Scalable Network Monitoring", ©2014 IEEE.

[7]Supeno Djanali, FX Arunanto, Baskoro Adi Pratomo, Abdurrazak Baihaq Hudan Studiawan, Ary Mazharuddin Shiddiqi, "Aggressive Web Application Honeypot for Exposing Attacker's Identity" , 2014 1st International Conference on Information Technology, Computer and Electrical Engineering (ICITACEE).

[8]Rajani Muraleedharan, and Lisa Ann Osadciw, "An Intrusion Detection Framework for Sensor Networks Using Honeypot and Swarm Intelligence", in Digital Object Identifier: 10.4108I/CST.MOBIQUITOUS2009.7084.

[9]Honeypot Project, "Know Your Enemy: Honeynets", in http://www.honeynet.org, last modified: 31 may 2006.

[10] Anagnostakis, K. G "Detecting targeted attacks using shadow honeypots." Proceedings of the 14th conference on USENIX Security Symposium. ACM, 2005. 129-144.