International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 1, November-December 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

# Honeypot Methods and Applications

**Anoop V Kanavi[1], Feon Jaison[2]**

[1]Student, [2]Assistant Professor,
[1,2]Master of Computer Application, Jain (Deemeed-to-be) University, Bangalore, Karnataka, India

**ABSTRACT**

Day by day the internet is becoming an essential part of everyone's life. In India from 2015 – 2020, there is an increase in internet users by 400 million users. As technology and innovation are increasing rapidly. Security is a key point to keep things in order. Security and privacy are the biggest concern in the world let it is in any field or domain. There is no big difference in cyber security; the security is the biggest concern worrying about attacks which could happen anytime. So, in this paper, we are going to talk about honeypot comprehensively. The aim is to track hacker to analyze and understand hacker/attacker behavior to create a secure system which is sustainable and efficient.

***KEYWORDS:*** *Honeypot, hacking, network security, forensic*

***How to cite this paper:*** Anoop V Kanavi | Feon Jaison "Honeypot Methods and Applications" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-1, December 2020, pp.725-728, URL: www.ijtsrd.com/papers/ijtsrd38045.pdf

IJTSRD38045



## 1. INTRODUCTION

Due to the increase in the growth of internet usage, people can easily access their information or transfer data to others on the internet. due to such a rapid growth of the internet, if we do not know the value of basic network security, which will lead hackers to take over the network by exploiting a vulnerability in the network by using malicious code. The attack may lead to stealing, tampering of information that leads to damages, and loss of data. We Traditionally use IDS (Intrusion Detection System) and Firewall in a network to prevent attacks and avoid damages that provide defense against the attackers. Firewall or IDS, you collect and analyze logs on your network, identifying malicious signatures or anomaly in a sea of legitimate activity can be both time consuming and difficult. Since it is hard to identify false positive and false negative.

A honeypot is a device that is built to monitor the network and analyze the attacker's behavior. A honeypot is a system that attracts attackers/hackers into it, by luring them into the system and make them run exploits and they fall into the trap. Honeypot lets you monitor the processes that are started and running on the system by the attacker. A honeypot is a trap machine that looks identical to the real system to attract the attacker/hacker. This device can also be used as a forensic device in a crime scene to identify hackers trying to steal the data. Honeypot won't completely screen off the hackers but rather notify us by telling there is an attack happening or attack which may happen. The main purpose of the device is to watching, analyze, understand, and tracking hacker's behavior so we can create a better and secure system.

## 2. Classification of Honeypot

Honeypot are broadly classified into two parts. One is according to their usage and other is according to their level of involvement. According to usage they are classified into two types

A. Research honeypot
B. production honeypot

According to their level of involvement they are classified into three types

A. low interaction honeypot
B. mid interaction honeypot
C. high interaction honeypot

### 2.1. Research Honeypot

As the name suggests, research honeypots are mainly used for research purposes. They are meant to gather maximum information about hackers or intruders by giving full access to the system. By allowing access it is easy to understand the behavior of the attacker and monitor which tools and methodology are implemented. The aim is to understand how attackers develop and progress to learn how to improve and secure our system. Research honeypots don't add any security to the organization, but they are used to help in understanding the hacker's community and their motives.

### 2.2. Production Honeypot

Production honeypots are placed inside the enterprise network along with the production servers. This type of honeypot is mainly used to protect the organization from any malicious attacks done by hackers. The honeypot plays as a decoy but it is designed to look and appear as real and contains information that attracts the hackers to spend time

and resources, ultimately giving system/network admin to assess and mitigate any vulnerability in their actual system. Production honeypot is used to reduce the risk to provide a better and secure business environment. Hence, they are largely used in organizations

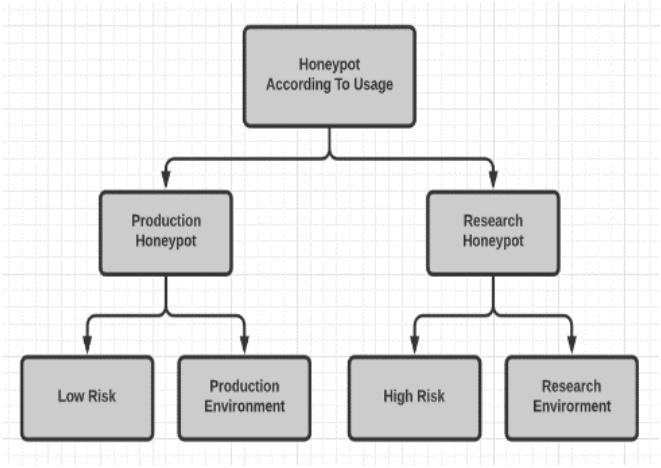


**Fig1. Honeypot According to Usage**

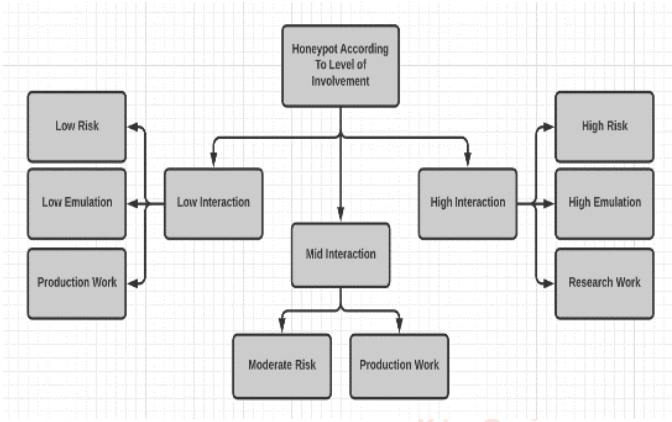


**Fig 2 Honeypot According to level of Involvement**

### 2.3. Low Interaction Honeypot

Low interaction honeypots are commonly used in the production network. It runs a handful of services and the freedom given to the attacker is minimum. It serves as an early warning mechanism. low interaction honeypot is passive in nature which limits the hacker from using the system to attack other systems. This type of honeypot is deployed keeping in mind to protect/secure ourselves from the attackers. In exchange, we get very little information about the hacker. so, this approach is widely used in organizations where their priority is to protect the system from any external attack.

### 2.4. Mid Interaction Honeypot

Mid interaction honeypot provides more services which offer hacker more ability to interact compared to low interaction honeypot. It emulates certain aspects of the application layer but doesn't provide any real operating system. The level of emulation provided to the attacker increases the risk also. The organization can expect certain activity and give a certain response. They work to stall the attacker to get more time to figure out how to properly react to an attack.

### 2.5. High Interaction Honeypot

High Interaction Honeypot is not meant to imitate the whole production network/system, but they do run most of the services the production network/system would run. This type of honeypot is given a real operating system to attack. It allows the organization to see hacker's behavior and methods, the main aim is to get maximum information about the hackers by allowing access to the whole system. This type of honeypot consumes a lot of resources and have to be maintained constantly, but is worth the findings.

## 3. Application and Deployment of Honeypot

Here we discuss its application in educational areas, with IDS and its implementation

### 3.1. Honeypots in Educational Resource

A lab has been set up at Brigham Young University for network security reasons for undergraduate and graduate studies called ITSecLab. They utilize this lab for following the analyzing traffic in the organization. This lab was planned exclusively with the end goal of examinations on network security by undergraduates. In this lab, they have actualized a honeypot in their lab to connect with hackers and investigate its uses as an instructive apparatus. The lab is planned as a separate Sandbox to fend off the noxious exercises from the lab. The honeypot is executed at Brigham Young University remembering the specific advantages, for example, it informs about the new dangers, making sure about the lab at a more significant level, learning the organization and security rudiments, and intently recognizes the blemishes. One more viewpoint becomes an integral factor while executing the honeypot, the legitimate issues that are the most significant part in usage since, supposing that the honeypot gets compromised and is utilized as zombie then the proprietor needs to endure the misfortune.

### 3.2. Honeypot with IDS

An Intrusion Detection System (IDS) separates between the traffic coming from different hosts and the hackers, at the same time facilitate the issues of throughput, inactivity, and security of the organization. From that point onward, we can introduce the consequences of a grouping of burden and their reaction time in the terms of execution and adaptability tests and propose different sorts of expected uses for such a framework. In IDS we may utilize two regular sort location levels known as Misuse detection and Anomaly detection. In misuse detection, the IDS investigate all the different sorts of data that have been gathered and coordinates it to a huge information base of signatures. In anomaly detection, the admin makes a standard, or we may state a typical organization traffic load, breakdown, protocol, and packet information. It screens the organization and looks at it to those baselines. IDS can be additionally classified into Network-based and Host-based. In network-based IDS, the individual traffic is investigated though in host-based IDS all the exercises of the host are analyzed. Honeypots can either be a host and additionally network-based, however, for the most part, they are not network-based as all interface activities are commonly performed over an organization. Its key utility is that it rearranges the Intrusion Detection issue of isolating anomalous from ordinary. Subsequently, any movement on a Honeypot can be quickly characterized as anomalous. Every part assumes a particular function in the usage of honeypot with IDS inside an organization. At first, the heap balancer gets the virtual IP address and checks whether the packet containing the packet has been fragmented, and afterward, it is reassembled. At that point, the load balancer opens a TCP connection with the IDS

Process and sends the data of the packet (less the headers) over that connection. IDS check the data of the packet against its database and returns the Boolean value of that to load balancer through a similar TCP connection. In the wake of accepting the outcome, the load balancer shuts the TCP connection. On the off chance that the outcome from the IDS was valid (Indicating an attack) the packet is sent to the Honeypot. otherwise, a server is chosen from the dynamic server pool in a cooperative design and the bundle is sent to the server.

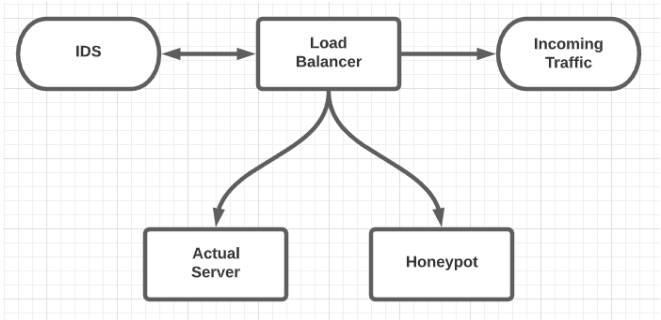


**Fig3 Flow of packets through IDS in Honeypot**

### 3.3. Network Security Through Hybrid Honeypot

A honeypot is a security asset whose worth lies in being examined, assaulted, or compromised. A honeypot is a framework that is made and set up to be hacked. It tends to be utilized in an alternate situation as an IDS, safeguard, or response component. Moreover, it can be sent to devour the assets of the attacker or divert them from the valuable targets and moderate them down that they waste their energy and time on the honeypot as opposed to assaulting production frameworks or servers. Here again, we partition the honeypots into two classifications as indicated by their degree of interaction, low-level interaction, and high-level interactions. The degree of interaction can be characterized as the greatest scope of assault prospects that a honeypot permits an attacker to have. In high-level interaction honeypot, hacker associates with working operating systems, all the programs and services and this sort of connection can be utilized to notice the hacker's behavior, their tools used, motive, and investigate vulnerability. This kind of high-level interaction honeypot can be set up in a virtual machine utilizing different virtualization programming, for example, VMware, Qemu, and Xen. An example of this honeypot is honeynet. It is a network of different frameworks. Honeynet can gather profound data about hackers, for example, their keystrokes when they exploit the system, their interaction with other hackers, or the different tools they use to investigate and create a defenseless system. On a low-level interaction honeypot, there is no working operating system that an attacker can work on. All the tools are set up to mimic OS and different services. Furthermore, they all work along with the attacker and malicious code. This will decrease the danger drastically. This kind of honeypot has a couple of possibilities of being undermined. These are production honeypots. Regular utilization of low-level interaction honeypot incorporates; port scan recognizable proof, age of assault signature, pattern examination, and malware collection.

### 3.4. Deployment of Intrusion Detection Signatures using Honeycomb

This generally deals with the generation of signatures. As of now, generating signature is tedious work, a manual process that necessities itemized information on every product work that should be kept. Oversimplified signatures will in general produce huge quantities of false positives, too explicit ones reason false negatives. For a similar explanation, the idea of Honeycomb a system that generates a signature for malicious traffic consequently is utilized. Here pattern detection methods and packet header are utilized for conformance tests on traffic caught by honeypots. The reason examined the attack signatures is to clarify the trademark components of attacks. At this moment we don't have any such norm for characterizing these signatures. As an outcome, various systems offer signature languages of changing expressiveness. A decent signature must be limited enough to keep decisively the characteristic parts of exploiting it attempts to address; simultaneously, it should be adaptable enough to catch varieties of the attacks. Disappointment in one manner or different prompts either a lot of false positives or false negatives. In this manner, the system underpins signatures just for the Snort NIDS. Snort's signature language is right now not as open. So, we incorporate Snort here due to its current standing and colossal signature stockroom. the system utilized here is an augmentation of honey a popular low-level interaction open-source honeypot. Honeyd mimics has with personage networking characters. It interferes with traffic shipped off non-existent has and utilizes the imitated frameworks to react to this traffic. Each host's characteristics can be designed as far as OS type and running organization administrations.

## 4. Conclusion

We have additionally examined different sorts of honeypots and their utilization with various usefulness perspectives. our objective was to comprehend their technique and how they are functioning to draw attackers towards the system. We found their security flaws to support specialists and organizations. A few organizations are utilizing honeypot frameworks to ensure the entire organization's security, and analysts are making experiments on their home network. As we know network security is exceptionally huge for all systems because any unprotected machine in an organization can be undermined at any time. We have additionally examined different sorts of honeypots and their utilization with various usefulness perspectives.

## 5. Reference

[1] Spitzner, L. 2002. Honeypots: Tracking Hackers. 1st ed. Boston, MA, USA: Addison Wesley.

[2] Mokube, I. & Adams M., 2007. Honeypots: Concepts, Approaches, and Challenges. ACMSE 2007, March 23-24, 2007, Winston-Salem, North Carolina, USA, pp.321 325.

[3] Know Your Enemy: Honeywall CDROM Roo 3rd Generation Technology, Honeynet Project & Research Alliance, http://www.honeynet.org

[4] Ram Kumar Singh & Prof. T. Ramanujam. Intrusion Detection System Using Advanced Honeypots, 2009

[5] The Honeynet Project. Know Your Enemy: Honeynets (May 2005) http://www.honeynet.org/papers/honeynet/.

[6] Honeynet Research Alliance. Project Honeynet Website. http://project.honey.org

[7] The Honeynet Project, Know Your Enemy: Honeynets, April 2001.

[8] The Honeypot Project, Know Your Enemy: Revealing the Security tools, tactic, and motives of Blackhats community.2002.

[9] Hybrid Honeypot System for Network Security by Kyi Lin Lin Kyaw, 2008.

[10] Spitzer, Lance. Honeypots, Tracking Hackers. Pdf version. Addison Wesely, 2002.

[11] Honeynet project. Know your enemy: Honeynets. http;//www.Honeynet.org/papers/honeynet/index.html

[12] Research infrastructures action, Sixth framework programme, D1.1: Honeypot Node Architecture, page 7-24.

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

[14] M. Roesch, Snort: Lightweight Intrusion Detection for Networks. In Proceedings of the 13th Conference on Systems Administration.