IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, January 2023
Impact Factor: 7.301

A Review on Honeypots

Mr. Pradeep Nayak[1], Sujan P S[2], Abhishek R Bhat[3], Sudheer[4], Mohammed Sufiyan[5]
Faculty, Department of Information Science and Engineering[1]
Students, Department of Information Science and Engineering[2,3,4,5]
Alva's Institute of Engineering and Technology, Mijar, Mangalore, Karnataka, India

Abstract: *Organizations and people alike are becoming increasingly concerned with information security today. Increasingly aggressive kinds of defense are becoming more popular as a result to enhance the current strategies. Utilizing honeypots is one of these strategies. A cyber security resource called a honeypot has value when it is probed, attacked, or compromised. To address the issue, all-around honeypots, which entail a major improvement in sensitivity, deception, and countermeasure, are required. In this paper, we give a brief overview of honeypots. It has become difficult to collect high-quality attack data in the context of honeypot areas due to the growing diversity and sophistication of cyberattacks. We look at several honeypot designs, honeypot ideas, and honeypot implementation strategies. Index Terms—Honeypot, cyber security, cyberattacks.*

Keywords: Honeypot

I. INTRODUCTION

The concept of trapping and tricking computer attackers in order to observe their behavior and divert them has been successfully implemented in the realm of computer security since the early 1990s. This technique, often carried out by using Honeypot, a computing system set up to simulate crucial resources, has exposed attacker tactics and protected more crucial computing resources [1]. As more attackers became aware of Honeypots, they created methods to find them. A number of security solutions are provided to lessen the risk, including firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS). A honeypot is a type of security facility that specifically aims to allow being attacked for the purpose of studying the creation of the hacker community by advertising/exposing its information systems resource to tempt unauthorized and illicit access, in contrast to these tools, which are primarily used to prevent attacks.The use of honeypots as an active component was motivated by an intriguing phenomenon in nature, which is illustrated by the way Japanese honeybees protect their beehives from mass hornet attacks. We describe how the giant hornets attack a colony of common honeybees in order to comprehend such a tactic (not the Japanese bees). A hornet first deposits its pheromone at the entrance to the hive. The pheromone draws in other hornets, causing them to arrive and assault the hive collectively. Since the hornets' armor prevents the honeybees' stingers from penetrating it, the honeybees are killed in large numbers; merely 30–40 hornets can exterminate 30,000 honey bees in a matter of hours. To repel the hornet attack, however, Japanese honeybees use an unusual defensive tactic. The honeybees manning the entrance would return to the hive when a hornet marked the entrance to the hive. Instead of letting them launch their attack from outside, this entices the hornet inside the hive. Over a thousand worker honeybees would simultaneously emerge from their combs and assemble in a mass immediately inside the hive's entrance. The bees surround the hornet and gather into a ball of bodies when it tries to enter the hive, cooking it to death with their body heat. They stop the pheromone from drawing in more hornets by killing the first few hornets. As a result, their hive is safeguarded by activating quick action in the face of hornet attacks.

Network decoys used as honeypots are closely watched and have the following functions:

1. They can divert attackers away from networked machines that are more valuable.
2. They can offer early notice of fresh attack and exploitation patterns.
3. They enable thorough investigation of adversaries both during and after honeypot exploitation [2].

The structure of this essay is as follows: We look at various honeypot kinds in Section 2. We give an overview of the honeypot idea and methods for their implementation in Section 3. Section 4 discusses the problems and legal implications related to honeypots. Finally, in section 5, we offer our assessment of the future of honeypots.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, January 2023
Impact Factor: 7.301

II. BACKGROUND AND RELATED WORK

One of the earliest instances of a honeypot being used in cybersecurity dates back to January 1991. While employed by AT&T Bell Laboratories on January 7, 1991, Cheswick saw a cracker—a criminal hacker—trying to copy a password file. Cheswick said that he and his associates built a "chroot "Jail" (or "roach motel")" that allowed them to keep tabs on their assailant for several months. In 2017, Dutch police used honeypot techniques to track down users of the darknet market Hansa. Police in the Netherlands killed and in possession of Hansa. It served as a honeypot to potentially identify thousands of users of the black market by watching them and stealing their login information, which represents perhaps the biggest victory for international law enforcement in their fight against the illicit online drug trade. More than 1,000 bitcoins, valued at about $2.6 million, were reportedly seized by Dutch police as part of the Hansa operation. The strategic factors to be taken into account when utilizing honeypots are discussed in some detail in several works. Attackers have become more interested in compromising the resources controlling these cyber-physical systems (CPSs) as the CPS space expands and becomes more networked. In response, honeypots have been created to look like CPS-specific components. Numerous papers have been written about specific aspects of honeypots and how they can be made and used as a result of this research.

2.1 Types of Honeypots

According to their purpose (production, research, and honeytokens) and degree of interaction, honeypots can be categorized (low, medium, and high). Honeypots can be categorized according to how they are used and how involved they are. Depending on their placement, honeypots can be categorized as:

- Production honeypots
- Research honeypots

2.2. Purpose of Honeypots

A. Production honeypots

Production honeypots are popular among businesses because they are simple to use, only gather a small amount of data, and are easy to use. In order to increase overall security, a company will install production honeypots alongside other production servers inside the production network. Production honeypots are typically low-interaction honeypots because they are simpler to deploy. Compared to research honeypots, they provide less information about the attacks or the attackers.

A. Research honeypots

To learn more about the goals and strategies used by the black hat community to target various networks, research honeypots are operated. These honeypots do not directly benefit any one company; rather, they are used to study the vulnerabilities that businesses face and discover new ways to defend against them. Research honeypots are employed mostly by government, military, or academic institutions and are difficult to deploy and manage while collecting a lot of data. [6]

2.3 Level of Interaction

Honeypots can be divided into categories based on the degree of interaction that is permitted between the intrusive party and the system in addition to being either production or research honeypots. Low-interaction, medium-interaction, and high-interaction are these categories. The degree of interaction that is appropriate for you will depend on what you want to do with your honeypot.

A. Low-interaction Honeypots

Only services that cannot be used to get full access to the honeypot are simulated in a low-interaction honeypot. There is no operating system for the attacker to interact with on a honeypot with limited interaction. This reduces the risk connected with honeypots but severely restricts the availability of low interaction honeypots. Multiple virtual machines can easily be hosted on a single physical system due to their low resource requirements, quick response times, and need

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, January 2023
Impact Factor: 7.301

for less code, which reduces the complexity of the security of the virtual system. However, they can still be employed as active worm defenses as well as spammer analysis tools.

B. Medium-interaction Honeypots

Just as low-interaction honeypots, they lack an operating system, but the mimicked services are technically more challenging. It is still unlikely that the system will be penetrated, even though the likelihood that an attacker will discover a security flaw rises. Since there are more things for the attacker to interact with, medium-interaction honeypots give the adversary a stronger illusion of an operating system. Therefore, more intricate attacks may be recorded and examined.

C. High-interaction Honeypots

These honeypots are the most cutting-edge type. Because an actual operating system is involved, they are the most difficult and time-consuming to build and carry the greatest risk. A high-interaction honeypot aims to give the attacker a real operating system to interact with, free from restrictions or simulations. As a result, this kind of honeypot offers more opportunities for information gathering because all acts may be recorded and examined. A high-interaction honeypot should be continually monitored to make sure it does not turn into a threat or a security flaw because the attacker has more resources at his disposal. A honeynet is an illustration of a high-interaction honeypot, and it is frequently employed in research.

2.4 Types of Honeypots based on Threats

Different honeypot designs can be utilized to detect various dangers. Based on the sort of threat that is handled, different honeypot definitions exist. Each of them has a place in a comprehensive and successful cybersecurity plan. Various ways of setting up honeypots for custom use cases can be seen. They are often advanced versions of the traditional honeypot made to fit their use case. Several use cases of honeypots include dark web, emails, databases, IoT, HTTP, SSH etc. We'll look at some of the setups of honeypot done by one of many

A. Spam Honeypot

Spammers take advantage of exposed resources such as open proxies and mail relays. These are email delivery servers that accept messages from everyone on the Internet, including spammers. To find spammer activity, some system administrators have developed honeypot applications that pretend to be these abusable resources. These honeypots give these administrators access to a variety of features, and the presence of such fictitious, exploitable systems increases the difficulty or danger of abuse. A potent defense against abuse from people who rely on high volume abuse can be provided via honeypots (e.g., spammers). These honeypots can provide bulk spam capture and show the abuser's IP address, allowing administrators to identify spammers' URLs and response techniques.

B. Database Honeypots

By setting up a database honeypot, you can see and study many attack strategies, including SQL injection, privilege abuse, SQL services exploitation, and much more. Databases are a frequent target for web attackers.

C. Malware Honeypots

To encourage malware attacks, a malware honeypot imitates software applications and APIs. Then, using the features of the infection, anti-malware software can be created or API vulnerabilities can be fixed.

D. Spider Honeypots

By establishing online pages and links that are only available to crawlers, a spider honeypot aims to capture web crawlers (also known as "spiders"). You can discover how to stop harmful bots and ad-network crawlers by detecting crawlers.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, January 2023
Impact Factor: 7.301

E. Email Trap

Email traps, often known as spam traps, bury a phony email address where only an automated email address accumulator can locate it. One can also think of an email address as a spam honeypot if it is only used to accept spam. Any message addressed to it will undoubtedly be spam because the address is only used as a spam trap. The term "honeypot" would be more appropriate for systems and methods used to identify or defend against probes than "spamtrap." Spam is "legitimately" delivered to its target using a spamtrap, just like non-spam email would. The source IP of the senders can be added to a denylist, and all communications that have the same content as those delivered to the spam trap can be automatically prohibited.

III. CONCEPT OF HONEYPOT

We now examine the fundamental ideas behind honeypots and its applications. Honeypots are digital network bait that lure in intruders through deceit while diverting them from legitimate production systems. When an attack is slowed down by a honeypot with multiple levels, there is a greater chance that it will be noticed and that the attempt to stop it will be successful. Applications for intrusion detection and logging can be installed within the honeypot to listen for and record illegal activities. With this knowledge, it will be possible to understand how the intruders operate and develop effective defenses. In conclusion, the basic idea of a honeypot is to get knowledge from the intruder's behavior.

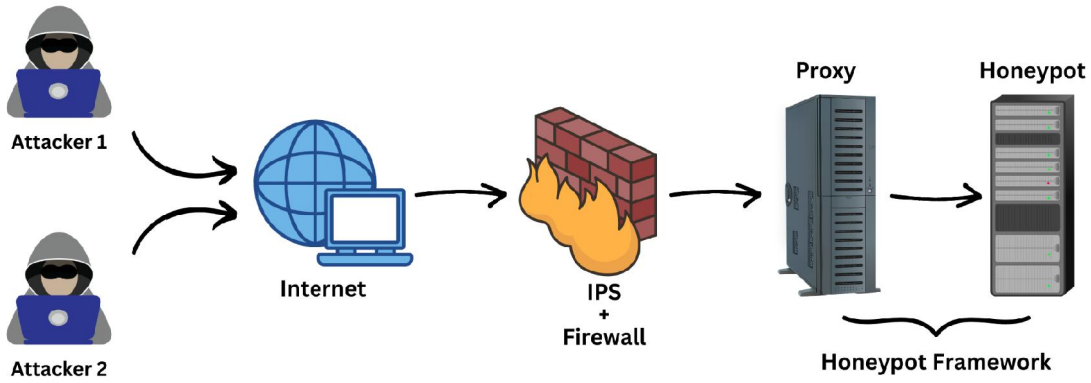
3.1. Implementations of Honeypot

Implementations of Honeypot include some factors that are needed to be considered:

- Realistic data must be used in order for the honeypot to pass for an authentic system. When the honeypot is compromised and the hacker uses the information against the organization, there are additional consequences to take into account. When such a situation occurs, plans must be in place to handle it.
- It is possible for an attacker to use a compromised honeypot to attack other systems; this is referred to as uplink liability.
- To avoid uplink liability, experts advise isolating the honeypot from your production system. [2]

3.2. High-Interaction Honeypot Framework

The purpose of our approach is to design and build a generic high interaction honeypot system that can detect application layer assaults automatically. Figure 1 displays a hypothetical scenario involving two attackers, a firewall / intrusion prevention system (IPS), and the honeypot framework. The IPS / firewall's aim is to filter incoming traffic for known attacks. A proxy and a honeypot host comprise the honeypot structure. The proxy host is in charge of session-individual logging of network traffic delivered to the honeypot. Furthermore, in the event that an attack is discovered, the proxy provides a way for replaying a specific previously logged session.



The replay mechanism built into the proxy can be used to thoroughly examine a detected attack and determine whether alternative system configurations are as vulnerable to the attack as the honeypot service. The honeypot host is made up of a honeypot service, which is actually a real service, and a host intrusion detection system (HIDS). The operating service is the bait that attracts worms or hackers, while the HIDS monitors the honeypot service. The implemented detection approach is general and can detect threats based on system-call signatures.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, January 2023
Impact Factor: 7.301

IV. ADVANTAGES AND DISADVANTAGES OF HONEYPOTS

Although honeypots have many advantages, there are also concerns and drawbacks.

4.1. Advantages

- Real data collection. Honeypots gather information from actual attacks and other unlawful activity, giving researchers a wealth of valuable data.
- Small data set. Honeypots are particularly concerned with the traffic that enters them. They are not worried about a network traffic overload or assessing the legitimacy of packets. Because of this, they only gather a little quantity of data; there aren't massive data logs or thousands of warnings per day. Despite the tiny size of the data set, the information is quite valuable.[2]
- Fewer False Positives. A honeypot decreases the amount of false positives because there is no motive for legitimate people to visit the honeypot, unlike standard cybersecurity detection technologies that can produce warnings with a high volume of false positives. [7]
- Economical. They need few resources because they solely record illegal conduct. A honeypot could be created using an outdated or low-end system. Because they only interact with malicious activity and do not need high-performance resources to process enormous volumes of network data in search of attacks, honeypots can be good investments.
- Honeypots are designed to catch whatever that is thrown at them, including new tools and strategies. Even if an attacker is using encryption, honeypots can still record illicit activities.
- Detect Internal attacks. Internal vulnerabilities can also be detected via honeypots. The majority of businesses are occupied with perimeter defense. However, if you merely protect the perimeter, any hacker who manages to get past your firewall is free to cause any harm they see fit once they are inside. Additionally, firewalls are useless against internal threats. A honeypot can show flaws in areas like permissions that allow insiders to hack the system and provide you with equally useful information on internal threats.

4.2. Disadvantages

- Short sighted. A honeypot only monitors and records activity when an attacker engages with it directly. Attacks on other system components won't be stopped until the honeypot is also in danger. There won't be any data to analyze if the honeypot isn't attacked. [7]
- Discovery and Fingerprinting. Experienced hackers can frequently tell a production system from a honeypot system using system fingerprinting techniques because honeypots may frequently be distinguished from legitimate production systems. A honeypot can be fingerprinted when an attacker can determine its true identity by observing certain predicted traits or behaviors. A honeypot can be identified by a small error, such as a misspelled word in a service emulation. [2]
- Risk of Takeover. The honeypot may be used to attack other systems inside or outside the company if it were taken over. The honeypot might be used to conceal and disseminate illegal substances. Despite being cut off from the main network, they eventually connect in some fashion so that administrators can get the data they contain. Because it seeks to tempt hackers to get root access, a high-interaction honeypot is often seen as riskier than a low-interaction one. [2]
- Legal Issues. There are many legal stumbling blocks that can make honeypot a liability. The usage of a honeypot may or may not be legal depending on a variety of conditions. The key contributing variables are entrapment and the right to monitor system users. [2]

V. CONCLUSION

In this paper, we have given a quick introduction to honeypots and discussed some of their applications. We've talked about the various kinds of honeypots, including production honeypots and research honeypots. We also studied the elements a honeypot implementation should take into account. For instance, the purpose you wish to use your honeypot

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, January 2023
Impact Factor: 7.301

for will determine the level of contact. We talked about the architecture of general high-level honeypot interactions. Finally, we considered the benefits and drawbacks of honeypots.

Honeypots can assist firms in keeping up with the always shifting threat landscape as cyber threats continue to emerge. Although it is hard to predict and stop every attack, honeypots can help an organization be ready and are possibly the best technique to catch an attacker in the act by providing important information. They are also an excellent source of knowledge for cybersecurity experts. We think they can be an effective tool in digital forensics investigations because they can be utilized to gather data on attackers and other threats. Overall, employing honeypots has many more advantages than disadvantages. Hackers are sometimes viewed as an invisible, far-off threat, but utilizing honeypots, you can see exactly what they're doing in real time and utilize that information to prevent them from obtaining what they want.

REFERENCES

[1]. S. Litchfield, D. Formby, J. Rogers, S. Meliopoulos and R. Beyah, "Rethinking the Honeypot for Cyber-Physical Systems," in IEEE Internet Computing, vol. 20, no. 5, pp. 9-17, Sept.-Oct. 2016, doi: 10.1109/MIC.2016.103.

[2]. Iyatiti Mokube and Michele Adams. 2007. Honeypots: concepts, approaches, and challenges. In Proceedings of the 45th annual southeast regional conference (ACM-SE 45). Association for Computing Machinery, New York, NY, USA, 321–326. https://doi.org/10.1145/1233341.1233399

[3]. W. Fan, Z. Du, M. Smith-Creasey and D. Fernández, "HoneyDOC: An Efficient Honeypot Architecture Enabling All-Round Design," in IEEE Journal on Selected Areas in Communications, vol. 37, no. 3, pp. 683-697, March 2019, doi: 10.1109/JSAC.2019.2894307.

[4]. "An Evening with BerferdIn Which a Cracker is Lured, Endured, and Studied". cheswick.com. Retrieved 3 Feb 2021

[5]. Thomas Brewster, "Forget Silk Road, Cops Just Scored Their Biggest Victory Against The Dark Web Drug Trade" Jul 20, 2017

[6]. Katakoglu, Onur (2017-04-03). "Attacks Landscape in the Dark Side of the Web" (PDF). acm.org. Retrieved 2017-08-09.

[7]. https://www.kaspersky.co.in/resource-center/threats/what-is-a-honeypot

[8]. L. Teo, Y. . -A. Sun and G. . -J. Ahn, "Defeating Internet attacks using risk awareness and active honeypots," Second IEEE International Information Assurance Workshop, 2004. Proceedings., 2004, pp. 155-167, doi: 10.1109/IWIA.2004.1288045.

[9]. Diebold, Patrick & Hess, Andreas & Schaefer, Guenter. (2005). "A Honeypot Architecture for Detecting and Analyzing Unknown Network Attacks". 245-255. 10.1007/3-540-27301-8_20.