International Journal of Engineering Research & Management Technology

ISSN: 2348-4039

Volume 9, Issue-6 November-December- 2022

Email: editor@ijermt.org www.ijermt.org

CUMULATIVE APPROACH WITH HONEYPOTS AS A PLAUSIBLE TRAP FOR BLACK HATS

Rahul Singh Chowhan
Ph.D. Student, Shyam University

Dr. Poonam Keshwani
Assoc. Prof., Shyam University

ABSTRACT

This article discusses Honeypot, a method for ensuring the safety of networks. The fundamentals of honeypots, as well as their applications in contemporary computer networks and the academic setting, are covered in this study. A honeypot is a network-attached machine that is put up as a decoy to draw cyber attackers and detect, deflect, and investigate hacking attempts to obtain unauthorized access to information systems. Honeypots are used to lure cyber attackers into the system so that researchers may examine hacking efforts. Honeypots work by essentially creating a copy of the original website or server so that attackers will believe they are targeting a real victim when they launch an attack on them. However, because the honeypot is actually a trap, it will record the method and ways in which the attacker carried out the attack and will keep a record of those methods as well as information about the attacker. In this piece of writing, both the benefits and the drawbacks are discussed. Honeypots are often used by large corporations as well as businesses that are actively engaged in the field of cyber security research in order to detect and protect against assaults coming from advanced persistent threat (APT) actors.

Keywords**:** Cyber Security, Honeypot, Honey net, Network Security.

INTRODUCTION

Internet use is increasing in tandem with the expansion of the world's population. Internet access has rapidly evolved into one of the most useful and widespread technologies in the modern world. The internet has brought the whole globe closer together. Internet connectivity is very necessary for businesses, schools, and almost all other sectors of today's economy. And the security over the internet is also the most significant problem since those who wear black hats are seeking for possibilities to sneak into systems and servers in order to launch attacks on them. Security is a big worry, and as a result, network security has become one of the most popular subjects. Each and every hour, some other region of the planet experiences a fresh cyberattack from somewhere else in the world. Therefore, companies and individuals are expending time, effort, and financial resources in order to ensure the network's safety.

Encryption, decryption, cryptography, intrusion detection systems, firewalls, and honeypots are just a few of the various methods that may be used to beef up the security of a network.

Encryption is a process that involves wrapping or enclosing data that is sent over the internet by using an algorithm in a way that makes it impossible for an adversary to access the data. Decryption is a method that is used in order to decode the data after encryption, and the decryption key will only be accessible to the person who has been granted authorization. A method known as cryptography is quite similar to encryption in that it prevents an attacker from reading the data with ease by having the sender encrypt the data and the recipient decode the data. An intrusion detection system is a mechanism that can detect both incoming and outgoing activity, as well as identify and report suspicious behavior that occurs inside a network. It does this by monitoring network traffic in both directions. A firewall is used to filter undesired data packets or signals that might have an adverse impact on the system.

Honeypot is a trap for attackers who attempt to assault the system by using the honeypot, firms or researchers may comprehend or learn the strategies that attackers use to breach the system. Honeypot is also known as a honey pot. If a corporation or researcher is successful in implementing a honeypot, then effectively it becomes a kind of future attack prevention since they would have gained information of various attack tactics and new attack methods.

RELATED

Tools used till now:

1) In 1997, One of the first honeypot solution was available in security by Fred Cohen's Deception toolkit 1.0
2) In 1999, Know Your Enemy was published.
3) In 2000/2001 many honeypot tools were developed and organizations started adopting the tools.
4) In 2002, Honeypots used to detect and capture the attacks and their information. It was also used for military purposes.

HONEYPOT AND ITS TYPES

Honeypot is a technical term that can be described as a trap or diversion system that is implemented in a system, server, or network with valuable data for hackers. The intention of the honeypot is not to catch red handed the black hat community, but rather to silently monitor their methods and techniques. Honeypots can be implemented in a system with valuable data. The primary purpose of a honeypot is to collect as much data as possible so that researchers can better understand the strategies used by hackers. Honeypots may also be categorized according to how they are deployed and the amount of interaction they have.

They may be divided into two categories according to their mode of operation:

1) Production honeypots

Honeypots for production are most often used in both large and small businesses. They seem to be the same living structure as the original structure of the company, which attracts hackers and leads them to assume that they have found a legitimate system on which to launch an assault. Honeypot production is simple to use, and it simply gathers the information that is relevant; it does not collect a comprehensive amount of data. Honeypots are used to gather data, which is then used by an organization's cybersecurity team to construct a defense against any future assaults. They are honeypots with a modest level of interaction. Honeypots for production mirror the actual production servers so that when they are attacked, the vulnerabilities and gaps in the real production server may be investigated and worked to solve. Honeypots for production can also be used to test new security measures.

2) Research honeypots

On the other hand, research honeypots are used in order to obtain an increasing amount of information on the attackers and the attacking strategies.

It is quite difficult to put them into action, and organizations do not see any immediate financial benefit from doing so. Honeypots are used for research and study purposes to learn about the different motivations behind assaults and the best ways to defend against them. Universities, the military, the government, and other organizations make extensive use of them.

CLASSIFICATION BASED ON LEVEL OF INTERACTIONS

1) Low-interaction Honeypots

Honeypots that need little user intervention are simple to set up in a system and may be installed in a variety of services, including TELNET, FTP, and others. Honeypots like this provide very restricted access to potential attackers. These are very low-risk options. These are only meant to detect and fool the attacker from the original system, and they prevent the attacker from getting any farther into the network. They are relatively simple to install and take care of overall. When it comes to new attacks and zero-day assaults, low-interaction honeypots are not very successful at all. These honeypots are useful for capturing known attacks, but when it comes to new attacks, they are not very effective at all. "Honeyd" is an example of a honeypot with low levels of user interaction.

Honeyd is a piece of open-source software that was developed by Niels Provos and distributed under the GNU General Public License. Honeyd is free to download and use. The first major release, 0.5, was made available in 2003, and the most recent version that I was able to locate was 1.5c, which was made available in 2007. Honeyd was not the first honeypot, but it rapidly became the most accessible and versatile one. It was also the first honeypot that was completely constructed for the general public.

2) Medium- interaction Honeypots

Interaction on a medium scale Honeypots provide a higher level of involvement than low-interaction games but not as much as high-interaction ones. When there is a minimal level of contact, more access and functionalities are offered to potential attackers. These are also built or deployed as an application directly to the operating system, and emulated services are more powerful than low-interaction because of this. As a result, the risk participation is greater. "Nepenthes" is an example of a honeypot with medium-level interaction.

Nepenthes: The emulation of vulnerable services is the key concept that underpins nepenthes. There are now two primary ideas in this field: honeyd scripts essentially imitate the required components of a service in order to trick automated tools or extremely low-skilled attackers. honeypots are a kind of honeypot that uses honeypot scripts. This makes it possible to install thousands of low-interaction honeypots in tandem, allowing for a large-scale deployment. However, this strategy does have certain drawbacks, such as the fact that honeyd cannot replicate more complicated protocols. For instance, a complete emulation of FTP data channels cannot be accomplished with honeyd. In contrast to this, high-interaction GenIII honeypots make use of a genuine system and do not need the emulation of a service in order to function properly. The lack of scalability is one of the issues with using this strategy. Because of the restrictions imposed by maintenance needs and hardware prerequisites, it is not viable to deploy many thousand of these honeypots.

The gap that exists between these two methods may be bridged with the assistance of the platform that nepenthe provides. It is possible to install several thousands of honeypots in tandem, and the needs for the hardware and maintenance are relatively minimal. This software allows us to install hundreds of honeypots in parallel in an effective manner and gather data on malicious network traffic.

3) High-interaction Honeypots

These sorts of honeypots are very complex and difficult to both build and put into operation. These need a lot of effort and time to keep up with and maintain. Because there are restrictions for attackers and the original operating system is given, the risk is considered to be high. Since attackers are provided with actual operating systems, it would not be difficult for one to breach the system. "Honeynets" is an example of a honeypot with a high level of interactivity.

Honeynets are formed when there are two or more honeypots connected to the same network. Honeynet is a collection of honeypots with a high level of interaction that is used to monitor a bigger, broader, and more diverse network when the monitoring capabilities of a single honeypot are insufficient. These Honeynets provide the attacker a legitimate operating system so they may communicate with one other. Because of the high level of contact, researchers and security specialists are better able to cope with the methods that attackers use to get into the system, as well as their motivations and the ways in which they communicate. These govern the traffic that comes into and leaves the network while also capturing it. Honeypots with a high level of engagement are used extensively in many businesses as a deterrent against unwanted visitors.

OBJECTIVES

1. To study honeypot trap for black hats
2. To study tactics of black hat community

PLACEMENT OF HONEYPOT IN NETWORK

Honeypots are often installed in a DMZ, which stands for "demilitarized zone" on a network. This strategy maintains its separation from the primary product network while at the same time ensuring that it is a component of that very same network as shown in figure 1. The port needs to be kept open so that the attacker would be drawn to it and tricked into thinking that it is not a trap.

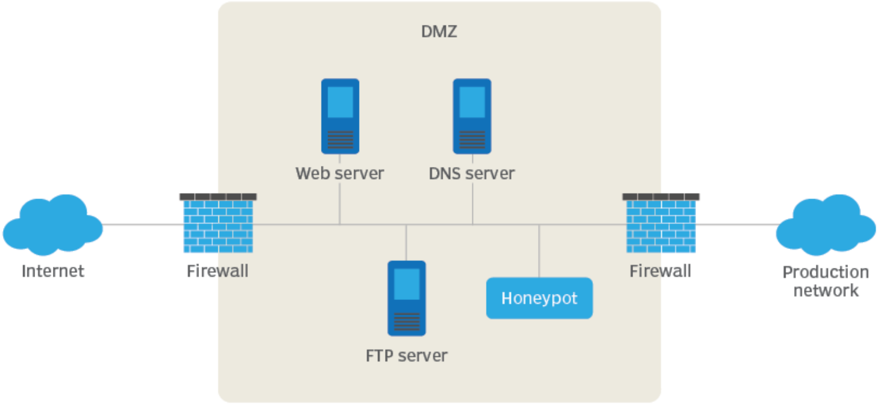

Fig -1: Honeypot place in network

A honeypot is a kind of decoy that is placed on a network to act as bait in order to attract potential attackers. Honeypots are often implemented as virtual machines that have been programmed to simulate the behavior of actual computers. They give the impression that they are operating complete services and applications and have open ports, much as a conventional computer system or server would on a network. The Honeypot is shown with a deeper hue in figure 2, which may be seen below.

In order to conceal its power, it has not been registered in any naming servers or any other production systems, such as the domain controller. This is significant because it is only inside a network that has been precisely set up that one can presume that every packet that has been delivered to the Honeypot is a suspect for an attack. If the packets are not in the correct order when they are delivered, the number of false alarms will rise, and the honeypot's effectiveness will suffer.

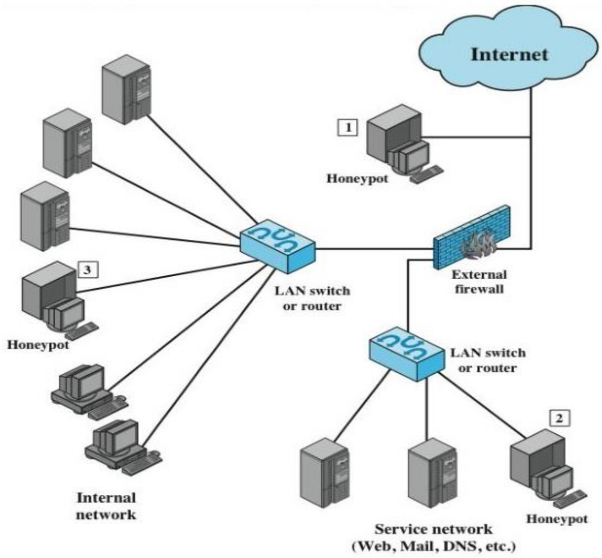

Fig. 2: Deployment Scenario of a Single Honeypot

DIFFERENT TYPES OF HONEYPOTS

Different types of Honeypots are

- **Email Traps:**

Email traps, often known as spam traps, are fictitious email addresses that are set up with the intention of collecting unwanted spam. Due to the fact that they are used to catch spam, they are not used for any other legitimate reason, and the emails that are received in that manner are entirely composed of spam. By doing so, the people and organizations gather data such as email addresses and IP addresses, which they then use to blacklist those email addresses and IP addresses in the future.

- **Decoy Database:**

It is possible to set up a fake database in order to monitor software vulnerabilities and identify attacks that exploit vulnerable system design or employ SQL injection, SQL services exploitation, or privilege abuse. These types of attacks may be detected using this method.

- **Malware Honeypot:**

Malware honeypots are designed to trick harmful programmes into giving up their sensitive information so that the vulnerabilities in the software may be patched or an antimalware programme can be developed using the information obtained.

- **Spider Honeypot:**

By producing online pages and connections that are inaccessible to humans, a spider honeypot serves the purpose of luring in web crawlers (also known as "spiders"). You may learn how to stop dangerous bots and ad network crawlers by detecting crawlers, which can also help you block ad network crawlers.

The researchers are able to learn the following by keeping an eye on the honeypot:

1) The origin of the assaults on the network
2) Have the ability to save the IP address
3) The degree to which dangers exist
4) What kinds of applications are of interest to them.

ADVANTAGES OF HONEYPOT

Honeypots provide a wide variety of benefits, each of which is unique. Honeypots focus primarily on the traffic that enters their networks and only collect limited amounts of data as a result. They gather a relatively small amount of the information that is impacting.

DISADVANTAGES OF HONEYPOT

Although they are uncommon, honeypots can come with a few potential dangers and drawbacks.

i) I Limited Vision - The only way honeypots are able to catch anything is when they are being assaulted themselves. They do not record any occurrences, though, while they are not being assaulted by anything.

ii) Discovery and Fingerprinting: Fingerprinting occurs when an attacker realizes they are being caught in a trap. Discovery is the process through which an attacker discovers an exploit. The attackers are kept on their toes by even minor slip ups.

iii) High level of Risk- In high-level interaction honeypots there is huge risk as it provides a real operating system.

CONCLUSION

Concerns about network security are growing on a daily basis with the development of new technologies and approaches. This article discusses ways to defend against assaults like this as well as the operation of honeypots. Honeypots may boost the effectiveness of other security mechanisms, such as intrusion detection systems (IDS), when used together. It is the only strategy that compels attackers to carry out their attacks while also gathering the information they need. Attackers were already aware that the honeypot was set up to entice them in; hence, subsequent improvements and tactics should be enhanced in such a manner that attackers are unaware that the honeypot is set up to catch them.

REFERENCES

[1]. IBM X-Force, 2013 Mid-Year Trend and Risk Report, CISO Security Insights, 2013.

[2]. K.Meenakshi, M.NaliniSri, "PROTECTION METHOD AGAINST UNAUTHORISED ISSUES IN NETWORK HONEYPOTS ", International Journal of Computer Trends and Technology (IJCTT), volume4, Issue4, 2013.

[3]. N.PROVOS, "A Virtual Honeypot Framework", In Proc. of 13th USENIX Security Symposium, 2004.

[4]. A.Rama Mohan Reddy, K.Munivara Prasad, and V Jyothsna," IP Traceback for Flooding attacks on Internet Threat Monitors (ITM) Using Honeypots", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.1, 2012.

[5]. C. Toinard, J. Briffaut, and J.-F.Lalande, "Security and Results of a Large-ScaleHigh- Interaction Honeypot ", JOURNAL OF COMPUTERS, VOL. 4, NO. 5,2009.

[6]. Vinu V Das, " Honeypot Scheme for Distributed Denial-of-Service Attack", IEEE, 2009 ,

[7]. 7- Yun Yang, Hongli Yang," Design of Distributed Honeypot System Based on Intrusion Tracking", IEEE, Communication Software and Networks (ICCSN), 2011, Pages: 196-198.

[8]. Divya, AmitChugh," GHIDS: A HYBRID HONEYPOT SYSTEM USING GENETIC ALGORITHM", International Journal of Computer Technology & Applications, , Vol. 3 Issue 1, 2012, p187-191

[9]. DasenRen, Juan Wang, and Qiren Yang, " An intrusion detection algorithm based on decision tree technology", IEEE, Asia-Pacific Conference on Information Processing , 2009,Pages: 333-335.

[10]. Jiqiang Zhai, Keqi Wang, “Design and Implementation of Dynamic Virtual Network", IEEE, Proceedings of 2011 International Conference on Electronic&Mechanical Engineering and Information Technology, Volume: 4 Pages: 2131-2134, 2011.

[11]. Narinder Kaur, "Honeypot", International Journal of Computing & Business Research,ISSN (Online): 2229-6166,2012

[12]. AlokS hukla, Kanchan Hans, "Honeypots : Fighting Against Spam", International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 1 Issue 3, May - 2012