Honeypot: A Trap for Black Hats

Menon Sanoop Govindankutty

Student, M. Sc IT, Keraleeya Samajam(Regd.) Dombivli's Model College, Maharashtra

---

Abstract - *This paper is about Honeypot, a technology for Network security. This paper deals with the basics of honeypots, how they are used in modern computer network and in educational world. [1]A honeypot is a network-attached system set up as a decoy to lure cyber attackers and detect, deflect and study hacking attempts to gain unauthorized access to information systems. Honeypot basically create a replica of original website or server where attackers think it is a genuine victim and performs the attack and compromise them, but as it is a trap the honeypot captures the method and ways how the attacker performed the attack and keep a track of that methods or attacker information. Advantages and disadvantages are mentioned in this paper. [1] Large enterprises and companies involved in cybersecurity research are common users of honeypots to identify and defend against attacks from advanced persistent threat (APT) actors.*

Key Words: Cyber Security, Honeypot, Intrusion detection system, Honeynet, Network Security.

1.INTRODUCTION

As world is growing internet is also growing day by day. Internet has become one of the power full and most needed tools in the world. Whole world connects over Internet. Companies, education and almost every industry is totally depended on internet. And the security over the internet is also the most important topic because the black hats are looking for the opportunities to get to attack the systems and servers. Network security is one of the hottest topics as security is a major concern. All over the world for every hour a new cyber-attack occurs in some other part of the world. So, the organizations and individual are spending the time, effort and money to secure the network.

There are many ways to powerup the network security like encryption, decryption, cryptography, intrusion detection system, firewall and honeypot.

Encryption is a technique where the data is shared through internet is wrapped or enclosed by using a algorithm so that the attacker cannot read the data. Decryption is a technique which is used to decrypt the data after encryption and the decryption key will be only with the authorised user. Cryptography is a technique which is similar to encryption where the attacker cannot easily read the data as the sender encrypt the data and receiver decrypt the data. Intrusion detection system is a technique used to detect the inbound and outbound of activity and detects the suspicious activity that occur in the network and inform. Firewall is used to block the unwanted income packets or signal which affect the system.

Honeypot is a trap for attackers who try to attack the system by the honeypot the companies or researchers can understand or learn the techniques used by the attackers to compromise the system. So, if a company or researcher successfully implement a honeypot basically it become a prevention for future attacks as they gain the knowledge of attacking methods and new attacks.

2. 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 where developed and organization started adopting the tools.
4) In 2002, Honeypots used to detect and capture the attacks and their information. It was also used in military purposes.

3. WHAT IS HONEYPOT?

Honeypot in technical term can be described as a trap, diversion system which is implemented in a system, server or network with valuable like data for hackers, whose intension is not catch red hand the black hat community instead silently monitor their methods and techniques. Honeypot is mainly used to gather the information as much as possible to study the methods used by hackers. Honeypot can also be classified based on deployment and on their level of interaction.

Based on deployment they can be classified into two:

1) Production honeypots

Production honeypot are mainly used in big and small organizations. They look like the same live structure like original structure of the companies which attract and make believe the hackers as it is genuine system to attack. It is easy to use and production honeypot only gather relevant information they did not collect vast information. The cybersecurity team of the organizations collects the data from honeypots and use that information to build a defense from future attacks. They are low interactive honeypots. Production honeypots mirror the live production servers and when they get attacked the vulnerabilities and loopholes are explored and can work on real production server to close those possibilities [2][3].

2) Research honeypots

In other hand research honeypots are used to gather more and more data from the attackers and attacking techniques.

They are very complex to implement and they are not directly profitable to organizations. Research honeypots are used to research, study about the various attacks motive and counter measure. They are mainly used by universities, military, government etc.

4. BASED ON LEVEL OF INTERACTIONS.

1) Low-interaction Honeypots

Low-interaction honeypots are easy to implement in a system and can be configured in services like TELNET, FTP etc. These kinds of honeypots give very limited access to attackers. These are very low-risk. These are just made to detect and deceive the attacker from original system and not allowing attacker to go in to depth. They are very easy to deploy and maintain. Low-interaction honeypots are not the effective enough, they are good to capture the known attacks but when it comes to new attacks and zero-day attack, they are not that effective. Example of Low-interactive honeypot is "Honeyd"

Honeyd: [4]Honeyd, the brainchild of Niels Provos, is free open-source software released under GNU General Public License. The first major release, 0.5, arrived in 2003, and the latest version I could track down, 1.5c, was released in 2007. Honeyd wasn't the first honeypot, but it quickly became the most accessible and flexible -- the first fully formed honeypot for the masses.

2) Medium- interaction Honeypots

Medium- interaction Honeypots are more interactive than low-interaction but not more than high-interaction. More access and functions are given to attackers than low-interaction. These are also implemented or installed as an application directly to the OS and emulated service are more powerful than low-interaction due to which the risk involvement is more. Example of Medium-interaction honeypot is "Nepenthes"

Nepenthes: [5] The main idea behind nepenthes is emulation of vulnerable services. Currently, there are two main concepts in this area: honeyd scripts simply emulate the necessary parts of a service to fool automated tools or very low-skilled attackers. This allows a large-scale deployment with thousands of low-interaction honeypots in parallel. But this approach has some limits: with honeyd it is not possible to emulate more complex protocols, e.g., a full emulation of FTP data channels is not possible. In contrast to this, high-interaction GenIII honeypots use a real system and thus do not have to emulate a service. The drawback of this approach is the poor scalability. Deploying several thousand of these honeypots is not possible due to limitations in maintenance and hardware requirements.

[5] The gap between these two approaches can be filled with the help of the nepenthe's platform. It allows to deploy several thousands of honeypots in parallel with only moderate requirements in hardware and maintenance. This platform
enables us to efficiently deploy thousands of honeypots in parallel and collect information about malicious network traffic

3) High-interaction Honeypots

These kinds of honeypots are very sophisticated and hard to develop and deploy. These are very time consuming and hard to maintain. There is restriction for attackers and original OS is provided and due to which the risk is high. An attacker could easily compromise the system as they are offered with real OS. Example for High-interaction honeypots is "Honeynets".

Honeynets: Two or more honeypots on a network from a honeynet [6]. Honeynet is a high-interaction honeypots which is used to monitor a larger and wider and more diversified network in which one honeypot is not sufficient. These Honeynet provide real OS to the attacker to interact with the attacker. This high-interaction helps researchers and security experts to deal with how attackers break in to the system their motive and how they communicate. These capture the inbound and outbound traffic in network and control it. This High-interaction honeypot is widely used in organizations to deal with the intruders.

5. WHERE TO PLACE HONEYPOT?

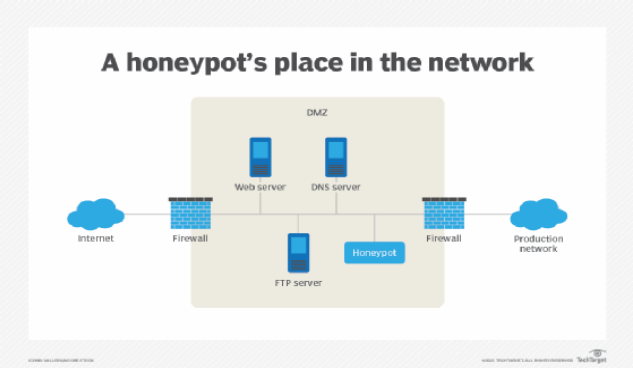

Fig -1: Honeypot place in network[7]

Honeypots are placed in DMZ- demilitarized zone on the network. This approach keeps it away isolated from the main product network but at the same time it is a part of the same network. The port should be left open so the attacker get attracted to it and make believe It is not a trap.

6. DIFFERENT TYPES OF HONEYPOTS?

Different types of Honeypots are

- **Email Traps:**

  Email Traps or Spam traps are fake email address created to trap spam mails. As they are used to trap

the spams they are not used for any other genuine purpose and the mails receiving in that are 100% spam mails. By this the organizations or individuals collects the data like mail id and IP address and they block that mail addresses and IP address in future.

- **Decoy Database:**

  A decoy database can be set up to monitor software vulnerabilities and spot attacks exploiting insecure system architecture or using SQL injection, SQL services exploitation, or privilege abuse [8].

- **Malware Honeypot:**

  A malware honeypot fakes the software or API, so that they get malicious and from that data the software loop holes can be closed or create an antimalware app.

- **Spider Honeypot:**

  A spider honeypot is intended to trap webcrawlers ('spiders') by creating web pages and links only accessible to crawlers. Detecting crawlers can help you learn how to block malicious bots, as well as ad-network crawlers [8].

By monitoring the honeypot the researchers get to know about:

1. Where the attacks are coming from
2. Can store the Ip address
3. The level of threats
4. What applications they are interested.

7. ADVANTAGES OF HONEYPOT?

Honeypots have various several distinct advantages.

i. Small Data Sets – Honeypots only pay attention to the traffic that comes to its network. They collect small portion of inform which is affecting the honeypot. There is no large data or capture big logs or 24 hours alert messages. But the small amount of data receive is highly valuable.
ii. Minimal Resources – Since it records only the bad activity, they need only minimal requirement.
iii. Simplicity – They are very simple and easy to maintain.
iv. Discovery of new tools and tactics- Honeypots capture the techniques and tools so if a new tools or techniques is captured in honeypot.

7. DISADVANTAGES OF HONEYPOT?

Honeypots have several risks and disadvantages, Although few.

i. Limited Vision – The only time the honeypots captures is when the honeypot gets attacked. But when they are not getting attacked, they do not capture any events.
ii. Discovery and Fingerprinting – Fingerprinting is when an attacker identifies they are getting trapped. Small mistakes make the attackers alert
iii. High level of Risk- In high-level interaction honeypots there is huge risk as it provides real operating system.

8. CONCLUSION

Network security concerns are increasing day by day as the methods and technique are evolving. This paper deals with countering such attacks and working of the honeypots. Honeypot can be used with other security mechanism such as IDS to increase efficiency. It is the only method where attacker are forced to do the attack and at the same time capture the information Attackers already knew that the honeypot is implemented to lure them so further improvement and techniques should be improved in such a way that attacker does not know that it is a honeypot.

REFERENCES

[1] https://www.techtarget.com/searchsecurity/definition/honey-po - What is Honeypot.
[2] "Honeypots" available at: https://en.wikipedia.org/wiki/Honeypot_%28computing%29
[3] R.Iyatiti Mokube, Michele Adams, "Honeypots: concepts, Approaches, and Challenges", Department of Computer Science, Armstrong Atlantic State University.
[4] Roger A. Grimes, "Honeyd: The open source honeypot," https://www.infoworld.com/article/2624595/honeyd--the-open-source-honeypot.html . ”
[5] Paul Baecher, Markus Koetter,ThorstenHolz, Maximillian Dornseif, and Felix Freiling: The Nepenthes Platform: An Efficient Approach to Collect Malware- https://www.researchgate.net/publication/225160275_The_Nepenthes_Platform_An_Efficient_Approach_to_Collect_Malware
[6] https://www.honeynet.org/papers/kye.html.
[7] https://www.google.com/search?q=Where+would+you+place+a+honeypot?&rlz=1C1CHBF_enIN980IN980&tbm=isch&source=iu&ictx=1&fir=sEH5sRPgGZxCjM%252CadY959mRU1Tf9M%252C_&vet=1&usg=AI4_-kQQLdBIbmteL_XW-HGQYvPKgDGxvw&sa=X&ved=2ahUKEwjs0siQlKv0Ah
[8] https://www.kaspersky.co.in/resource-center/threats/what-is-a-honeypot