Honeypot in Network Security

[1]Dr Devika Rani Dhivya K, [2]Thiruvenkatanath.M, [3]Prajith Kumar R

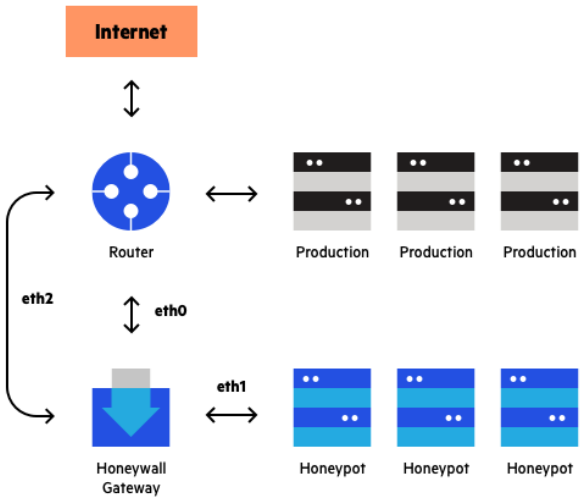
[1]M.Sc,M.Phil,MBA,Ph.D, [2,3]M.Sc SS
Sri Krishna Arts And Science College

Abstract: In reviewing the literature, it became apparent that the research can be new types of broken down into five major areas , honeypots to cope with emergent new security threats, utilizing honeypot output data to improve the accuracy in configuring honeypots to reduce the , threat detections, cost of maintaining honeypots as well as to improve the counteracting honeypot , accuracy in threat detections, legal and ethical issues in ,detections by attackers, and using honeypots.

1. Introduction

Network security is becoming increasingly critical to personal computer users, businesses, and the military. Security became a big concern with the development of the internet, and understanding the history of security offers a better understanding of the creation of security technologies.[5] Many security concerns were made possible by the internet's structure.

When the internet's design is adjusted, it can restrict the number of possible assaults that can be sent through the network.Understanding the attack mechanisms enables adequate security to evolve. Network security in the realm of networking refers to the provisions and policies implemented by the network administrator to prevent and monitor unauthorised access, abuse, modification, or denial of the computer network and network-accessible resources.Network security is the authorisation of data access in a network that is regulated by the network administrator. [4] Users, for example, choose or are issued an ID and password or other authenticating information that grants them access to information and programmes under their control. Other approaches for network security include cryptography, encryption-decryption, biometrics, firewalls, intrusion detection systems (IDS), and honeypots.



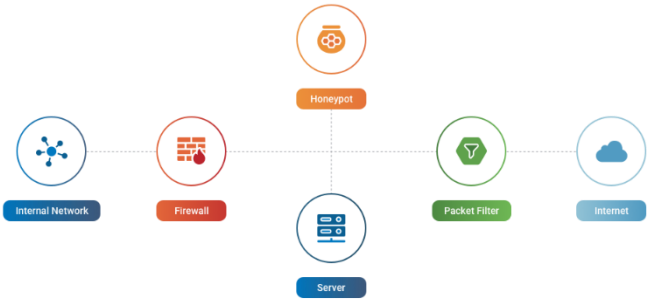
Encryption: The process of converting a plaintext communication into an encoded message known as Ciphertext.
Decryption: The process of recovering the original data from encrypted data.Prior to the contemporary era, encryption was virtually synonymous with the transfer of information from a readable state to seeming gibberish.
IDS (intrusion detection system):
It examines all inbound and outgoing network traffic for abnormal patterns that may signal a network or system attack by someone attempting to break into or compromise a system [8],[11].
Firewall:A mechanism that controls network access between two or more networks.
Biometrics: This technology uses a specific set of a person's vital data to identify identification.
Honey pot:A computer security system on the Internet that is specifically designed to attract and "trap" those who attempt to hack into other people's computerssystems.

2. What Is Honeypot?

A honey pot is a computer system that is specifically designed to attract and "trap" persons who attempt to hack into other computers (This includes the hacker, cracker). It includes some relevant data or, on occasion, behaves like a true operating system to the attacker, allowing it to be examined or assaulted. It serves as a decoy. The intruder's goal is to detect the Honeypot and attempt to break into it. A Honeypot's objective is to detect and learn from assaults, and then utilise that information to improve security.

3. The core technology of honeypots

Honeypot, as a component of an intrusion detection system, is mostly employed in network spoofing technology, based on data to capture information, regulate intruder access, and other technologies in the overall defensive system [6]. Honeypot core technologies include data management, data gathering, and data analysis.



3.1 Internet spoofing software

A honeypot is also known as a decoy assault technique.[7],[9] Only the invader may assault it in order to display its worth. The primary function of network spoofing technology is to identify the intruder's offensive methods, obtain their offensive goals, and cost the intruder a significant amount of time and money to secure the actual network.Honeypot technologies now comprise a variety of such deceptions, such as IP address spoofing, simulation system flaws enticing assaults, network traffic simulation, dynamic port configuration of the system, and so on.

3.2 Data analysis

The major purpose of the honeypot system is data analysis; the ultimate objective of our honeypot system setup is data analysis [12].The logarithmic analysis of the honeypot system is primarily concerned with the characteristics of the attack behaviour, which is also a difficult problem of the honeypot system, because the honeypot collects a large amount of information with no necessary connection between the information. If we want to better analyse the information, we need to establish a data analysis module to analyse the information, so the attacker establishdata analysis model.

3.3 Data gathering

The honeypot design of the core module refers to data collecting as the honeypot to monitor all actions to record. [1] It is difficult for us to gather as much danger as feasible throughout the intrusion detection phase. The more information we collect, the better we will be able to assess these assaults, including the attacker's purpose, approach, and tool.

3.4 Data management

Data control can reduce network intrusion, reducing the possibility of attackers using honeypots to attack or harm non-honeypot systems. We must make every effort to guarantee that after an attacker has penetrated our honeypot system, the impact to the non-honeypot system is minimised. We can only reduce the risk; different data control approaches and processes have varying degrees of danger; we cannot, however, entirely remove the risk.

4. Honeypot Classification

A. Depending on the amount of interaction

Honeypots are classed according on the amount of interaction between the invader and the system. There are three types of honeypots: low-interaction, high-interaction, and medium-interaction.

- **Low-interaction honeypots:**

These honeypots have a limited range of interaction with the outside world.[10] This form of honeypot is illustrated by FTP. There is no operating system for attackers to communicate with, but they use software to simulate characteristics of a specific operating system and network services on a host operating system to entice or identify attackers. The key benefit of this form of honeypot is that it is simple to deploy and maintain and does not require any sophisticated design. This method has certain advantages, but it also has some disadvantages. That is, it will not appropriately respond to exploits. This limits the capacity to assist in the discovery of new vulnerabilities or attack tactics.

- **High-interaction honeypot:**

The most sophisticated honeypot is the high-interaction honeypot.This form of honeypot interacts with the invasive system at a much higher level. It provides attackers with more realistic experience and accumulates more information about intended assaults; yet, there is a very high danger of capturing the entire honeypot. High-interaction honeypots are the most difficult to design and manage. High-interactivity honeypots are more beneficial when we need to record details about vulnerabilities or exploits that are not yet known to the outer world. This honeypot is ideal for "zero-day" assaults. Honeynets, for example, are often employed for research purposes.

- **Medium-interaction honeypot:**

Medium-interaction honeypots are often referred to as mixed-interaction honeypots. Medium-interaction honeypots are slightly more complicated than low-interaction honeypots, but less so than high-interaction honeypots. It gives the attacker a better illusion of the operating system, allowing more complicated attacks to be logged and analysed. Honeytrap, for example, dynamically constructs port listeners depending on TCP connection attempts taken from a network interface stream, allowing it to handle some unexpected assaults.

B. Based on the purpose

Honeypots are split into two types based on their purpose: research honeypots and production honeypots.

- **Research honeypot: [2],[3]** Research honeypots are mostly used to study new attack strategies and tools.Research honeypots are used to acquire intelligence about broad dangers that organisations may encounter, allowing them to better protect

themselves against those threats. Its primary objective is to gather information on the attackers' progression and attack lines. Honeypots for research are difficult to create, install, and administer. They are mostly utilised by institutions such as colleges, governments, armed forces, and intelligence agencies to learn more about dangers.Honeypot research provides a solid platform for studying cyber-threats and forensic abilities.

- **Production honeypot:** Production honeypots serve just to secure the network. Production honeypots are simple to design and deploy since they require few features. They safeguard the system by detecting assaults and alerting administrators. It is usually employed within an organisation to defend the organisation.

5. Conclusion

A honeypot is a valuable tool for attracting and trapping attackers and collecting data. Security is a vital component of every organization's website, but because honeypots based on hardware configurations are prohibitively expensive for small and medium-sized businesses, a software-based honeypot may be demonstrated to be a highly effective security solution for smaller businesses. Low-interaction Honeypots are the most often utilised Honeypots since they are simple to build and administer. High-interaction Honeypots, on the other hand, are the most secure and efficient Honeypot kind. These honeypots offer security as well as produce a log of all system entries, which is particularly useful in locating intrusive activities in the system.However, the honeypot must be upgraded to new techniques and assaults at some point in order to give security against new types of attacks. It is not a complete solution, but it is an excellent compliment to the security system.

References

1. Lanza Spitzer, “Know Your Enemy: Honeywell Comoro 3rd Generation Technology”, 2005.
2. Christian During, “Improving network security with honeypot.”
3. The Government of the Hong Kong Special Administrative Region, “Honeypot security” February 2008.
4. Honeypots: Basic Concepts, Classification and Educational Use as Resources in Information Security Education and Course
5. http://project.honeynet.org/papers/individual/Doering.pdf
6. http://security.rbaumann.net/download/honeyd.pdf
7. Setting Up And Running A Honeypot – Nepenthes, Brian Allen (baleen at wustl.edu) Network Security Analyst ,Washington University in St. Louis
8. http://www.pixel-house.net/midinthp.pdf [9]http://www.honeypots.net/.
9. http://www.honeynet.org/papers/kye.html.
10. http://www.honeyd.org/background.php. [12]http://cs.millersville.edu/~csweb/lib/userfiles/honeypot.pdf