Deceptive Defense: An in-depth Analysis of Honeypot Systems in Modern Network Security

Shrutika Sawai; Vaishnavi Bhongale; Darshan Khirekar
Master in Computer Application, Nagpur University, India

Abstract

In the modern digital age, network security is a big worry. The ongoing attempts by cybercriminals to take advantage of system flaws make improved security measures crucial. A honeypot is a unique security technique used to draw in attackers and observe how they behave. Security professionals use honeypots to improve defences by tricking attackers into disclosing their tactics by posing as legitimate systems.

This essay gives a general review of honeypot systems, covering their varieties, advantages, and disadvantages. Additionally, it describes the ways in which honeypots and intrusion detection systems (IDSs) cooperate to improve network security. Furthermore, we go over honeynets and Honeywell's, which improve the functionality of honeypots. Businesses may safeguard their networks from online threats by being aware of these technologies.

Keywords:
Honeypots, Intrusion Detection System (IDS), Network Security, Honeynets, Cyber Attacks

Introduction

In the modern digital world, network security is more crucial than ever. Cybercriminals are always trying to get into systems, steal information, or do harm. Security professionals employ a variety of tools and strategies to defend against these threats. The honeypot is one usefultool.

A honeypot is a phony system intended to draw in hackers. It is a trap, even though it appears to be a legitimate computer or network. Security professionals can observe the actions of hackers, gain insight into their strategies, and strengthen defenses when they attempt to attack it. Honeypots, in contrast to standard security tools, do more than merely stop attacks; they also provide insight into the motivations and methods of attackers.

In this essay, honeypot systems are discussed along with their role in network security. We discuss the advantages and disadvantages of the various types of honeypots. We also discuss how honeypots improve security by helping IDSs. We also discuss more sophisticated honeypot technologies such as honeynets and honeywalls for better security. Honeypots' concepts and usage can assist organizations in enhancing the security of their systems and defending them against cyberattacks better.

As the sophistication of cyberattacks increases, it is sometimes impossible to protect the organization's assets with basic measures like firewalls and antivirus software. It is therefore crucial for organizations to take proactive security measures as hackers are always coming up with new ways of circumventing security measures. Honeypots are used as a decoy to lure attackers into a trap that is actually a secure environment and whose activities can be closely monitored.

The collection of data on cyber attacks in real time is one of the greatest strengths of honeypots. They are designed to mimic bad behavior, so security professionals

DOI: https://doi.org/10.5281/zenodo.15610206

can use them to study attack patterns, virus behavior, and hacking techniques. This information can be employed by organizations in order to strengthen their security measures and stay one step ahead of the fraudsters.

Methodology Honeypots

One special security tool that is used as part of an organization's security measures is the honeypot. You would like the black hat folks to use these materials. In essence, a honeypot is an IT resources that is valuable only when used illegally or without authorisation . It implies that the threats utilising honeypots might be used to determine their value. If an attacker doesn't engage with honeypots, they aren't very useful. Honeypots do not, in fact, address certain issues. They can be employed as early warning systems, automating and slowing down attacks, and detecting new exploits to obtain information about new dangers. Honeypots can available in a variety of styles and sizes. They could be a simulated Windows application or a whole network that is vulnerable to intrusions like honeynets. Additionally, honeypots don't even need to be computers. These could be Excel spreadsheets, credit card numbers, or login credentials (They also called honey tokens).

Additionally, honey pots are available in a variety of designs and sizes. They are capable of imitating Windows-based applications and compromising and attacking large networks, like honeynets. Furthermore, honey pots aren't even required to be computers. These might be login credentials, Excel spreadsheets, or credit card numbers.

Types of Honeypots

1. Interaction-level based honeypots:

1.1. Low Interaction Honeypots:

The least amount of information is provided by low interaction honeypot systems. The sole purpose of its use is to record harmful data. As there is less data, there is less risk. Compared to the other two, these systems are simpler to install and set up. The actual operating system is not included. All they do is copy operating system services. One example of this type of honeypot is Honeyd.

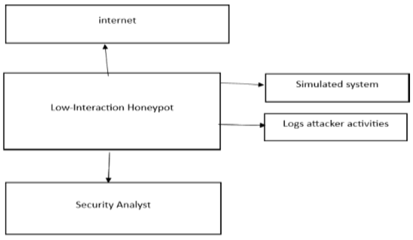


Fig 1: Low Interaction Honeypots

1.2. Medium Interaction Honeypots:

Honeypots with medium interaction have more capabilities than those with low interaction, but less than those with high involvement. Operating systems are absent from them. They have certain security flaws but are less complex than the high interaction ones. The hacker attacks the system as a result. Examples of medium interaction honeypots include Mwcollect, honeytraps, and Nepenthes.

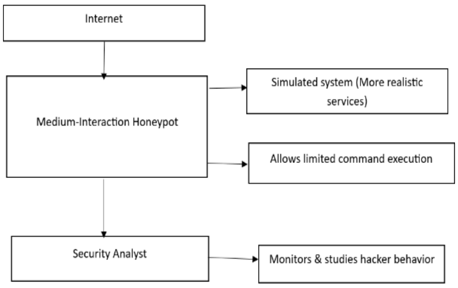

Internet
Medium-Interaction Honeypot
Simulated system (More realistic services)
Allows limited command execution
Security Analyst
Monitors & studies hacker behavior

Fig 2: Medium Interaction Honeypots

1.3. High Interaction Honeypot

As they engage more, high interaction honeypots typically gather a lot of data. These kinds of systems are riskier, though, because they provide hackers access to a lot of information. They are intricate and challenging to construct and maintain. Giving the

DOI: https://doi.org/10.5281/zenodo.15610206

attacker access to an authentic operating system with no restrictions or emulation is the goal of high-interaction honeypots. This technique is the most effective since it offers numerous chances to find different threats and weaknesses. One example of this kind of honeypot is Argos.

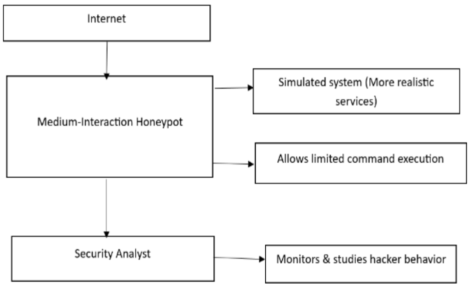
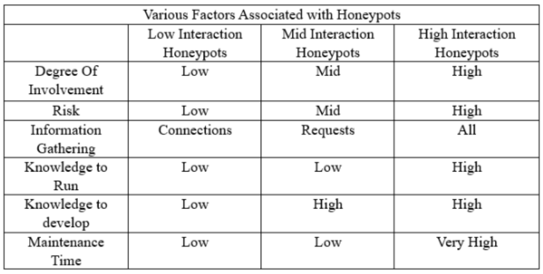

Internet
Medium-Interaction Honeypot
Simulated system (More realistic services)
Allows limited command execution
Security Analyst
Monitors & studies hacker behavior

Fig 3: High Interaction Honeypots

Table 1: Various Factor Associated with Different Honeypots.



Various Factors Associated with Honeypots			
	Low Interaction Honeypots	Mid Interaction Honeypots	High Interaction Honeypots
Degree Of Involvement	Low	Mid	High
Risk	Low	Mid	High
Information Gathering	Connections	Requests	All
Knowledge to Run	Low	Low	High
Knowledge to develop	Low	High	High
Maintenance Time	Low	Low	Very High

2. Purpose Based Honeypots:

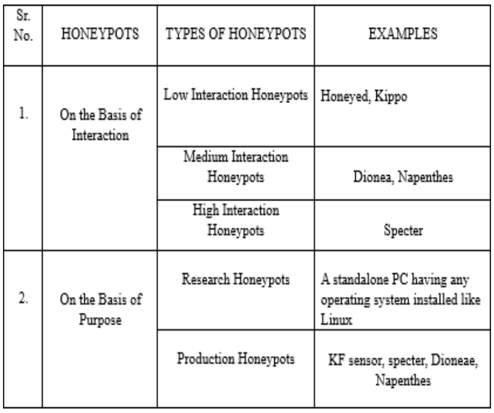
2.1. Research Honeypots:

Government, military, and research organisations employ research honeypots. They are especially employed for research in order to identify possible risks to the organisation. They offer information on attack patterns, profiles, the identity of the attacker, the tools used to launch the attacks, the attacker's motivation, communication habits, and more. To gather information on intruders, research honeypots delve deeper into the system. To find out more about the attackers, they simulate the operating system's actual environment. These systems are extremely risky and complicated. Additionally, it takes an administrator more time and effort.

2.2. Production Honeypots:

Production honeypots are employed to safeguard a company or organisation. They are put into place to safeguard and preserve the environment. They also lessen the hazards and attacks. The police enforcement of honeypot technologies are production honeypots. Commercial organisations employ production honeypots to lower the danger of attacks. Deployment, implementation, and maintenance of these systems are simple. They pose less risk because they are straightforward and have fewer features. Due to their functionality, production honeypots only offer a certain amount of information. They are only able to offer information about the affected systems and the exploits that hackers use. They don't provide information regarding the tools or attack profiles that were employed. Compared to research honeypots, they typically offer less information and have lower engagement rates.

Table 2: Type of Honeypots



Sr. No.	HONEYPOTS	TYPES OF HONEYPOTS	EXAMPLES
1.	On the Basis of Interaction	Low Interaction Honeypots	Honeyed, Kippo
		Medium Interaction Honeypots	Dionea, Napenthes
		High Interaction Honeypots	Specter
2.	On the Basis of Purpose	Research Honeypots	A standalone PC having any operating system installed like Linux
		Production Honeypots	KF sensor, specter, Dioneae, Napenthes

3. Advanced Honeypot System:

3.1. Honeynets:

A collection of different honeypots is called a honeynet. These are unique

DOI: https://doi.org/10.5281/zenodo.15610206

networks created to entice the assailants. A honeynet's purpose is to gather data regarding malicious activity. The investigators subsequently examine this recorded data to obtain the pertinent information. High-interaction honeypots are called honeynets. They behave like any honeypot and are incredibly adaptable. Since it will take them enough time to identify the phoney system, they can easily mislead any blackhat. Almost any operating system and program can be used on a honeynet.

3.2. Honeywalls:

One way to describe the honeywall is as a transparent bridge that prevents malicious data from leaving the honeynet. This stops other honeynet systems from becoming damaged. As a result, honeywalls regulate data and monitor outgoing traffic**.**

Characteristics Of Honeypots:

i. Honeypots are important for stopping harmful activity and attacks.
ii. It enhances response and assault detection times.
iii. It extracts the profiles of intrusion behaviour, system behaviour, and attack tactics.
iv. It catches the adversary's patterns of behaviour.
v. It logs every action taken by the intruder.
vi. They can be set up virtually or deployed physically.
vii. There should be no false alarms in honeypots.

Advantages Of Honeypots:

As the Honeypots are the part of Network Security. They have many advantages. These advantages are as follows:

- **Tiny data sets:**

  Any interaction with the honeypot is interpreted as malevolent. Thus, the thousands of alarms that were recorded by It is possible to decrease organisations to hundreds of entries.

- **Decreased False Positives:**

  The use of honeypots makes false positives less common. The less probable a security resource is to generate false positives or false warnings, the less likely it is to be used. Since any behaviour involving the honeypot is deemed risky, it is effective at identifying attacks.

- **Catching False Negatives:**

  Since each connection made to a honeypot is regarded as unauthorised, it is quite simple to catch false negatives with the aid of honeypots. Conventional attack detection technologies, such as signature-based detection tools, are unable to identify emerging threats. These tools only identify attacks that have already been identified by

- **Encryption:**

  If the harmful action is in encrypted form, honeypots can record it. Probes with encryption and

  Attacks engage with honeypots as a final destination where the honeypot decrypts the activity.

- **Utilising IPv6:**

  Hoeypots are compatible with IPv6 and any other IP environment. Countries like Japan and the Department of Defence actively employ IPv6, the latest version of IPv4. Numerous modern technologies, such as firewalls and ID sensors, are incompatible with IPv6.

DOI: https://doi.org/10.5281/zenodo.15610206

- **Adaptable:**
  Honeypots can be used in a wide range of settings. from an embedded social security number into a database or a whole computer network that is intended to be compromised.

- **Low Resource Requirements:** Honeypots need very little. Millions of IP addresses can be monitored with a basic Pentium computer.

Disadvantages Of Honeypots:

The disadvantages of honeypots are as follows:

- **Single Data Point:**
  Honeypots typically have the major disadvantage of being useless if no one attacks them. Of course, they can perform amazing things, but it will be blissfully unaware of any illegal activities if the attacker doesn't transmit any packets to honeypots.

- **Danger:**
  Honeypots have the potential to endanger an organization's environment once they are compromised. The risk associated with different types of honeypots varies. Honeypots with low interaction Honeypots that provide low risks but significant contact expose the attacker to enormous dangers, maybe affecting the entire platform. A badly managed honeypot can occasionally endanger the network as a whole. Additionally, honeypots don't work as intended until you have the time to use them correctly. Therefore, an administrator with in-depth understanding should carry out administration correctly.

Conclusion

In this paper, we have discussed about the honeypots in network security, Types of honeypots, its characteristics and advantages and disadvantages of honeypots.

In network security, the use of honeypots is a highly conventional practice. Information security now requires luring attackers to other fraudulent websites in the network as opposed to the website itself, which offers genuine information resources. These honeypots may even be expanded into honeynets, where an attacker would have to cope with a number of honeypots. The log files examined by these honeynets and honeypots could be utilised to improve the intrusion detection system and increase its intelligence in identifying intrusions.

References

[1] Spitzner, L. Open Source Honeypots: Learning with honeyd, Security
Focus.

[2] Kreibich, C. and Crowcroft, J. Honeycomb – Creating Intrusion
Detection Signatures Using Honeypots Proceedings of the Second Workshop on Hot Topics in Networks (Hotnets II), Boston,
51-56.

[3] Karthik, S., Samudrala, B. and Yang, A.T. Design of Network Security Projects Using Honeypots. Journal of Computing Sciences
in Colleges.

DOI: https://doi.org/10.5281/zenodo.15610206

[4] JohnCarroll, Computer Security, 3rd ed., Butterworth-Heinemann.

[5]A. N. Singh and R. Joshi, "A honeypot system for efficient capture and analysis of network attack traffic," in International Conference on Signal Processing, Communication, Computing and NetworkingTechnologies (ICSCCN).

[6] http://www.infoworld.com/d/security/beyond-honeypots-it-takeshoneytoken-catch-thief-216467

[7] Netsec. (2012, 15th March). Specter. Available: http://www.specter.com/default50.htm

[8] Baumann, R. and Plattner, C. White Paper: Honeypots, Swiss Federal Institute of Technology, Zurich.

[9] Craig Valli, Honeyd-OS artifice Australian Computer, Network & InformationForensics Conference.

[10] Wikipedia. http://en.wikipedia.org/wiki/Honeypot_(computing).

[11] Sutton Jr., R.E. DTEC 6873 Section 01: How to Build and Use a Honeypot.

DOI: https://doi.org/10.5281/zenodo.15610206