HoneyPot : Enhancing Cybersecurity through a computer simulation technology

Zhengchun Zhou * , and Wenyao Shen

College of Information Engineering, Shaoyang University, Shaoyang 422000, China

* Corresponding Author Email: 20156@hnsyu.edu.cn

Abstract. Honeypot technology is essentially a technique of deceiving attackers by deploying hosts, network services, or information as bait to lure them into attacking. This allows for the capture and analysis of attack behavior, speculating on attack intentions and motivations, enabling the defense to have a clear understanding of the security threats they face, and enhancing the security protection capabilities of the actual system through technical and management measures. A honeypot is like an intelligence gathering system. It is also possible to eavesdrop on the connections between hackers, collect various tools used by hackers, and gain control of their social networks.

Keywords: Honey Pot, cybersecurity, computer simulation

1. Introduction:

In today's digital age, cybersecurity [1] has become a paramount concern for individuals, businesses, and governments alike. With the increasing sophistication of cyber threats, traditional security measures alone are no longer sufficient to protect sensitive data and systems. As a result, innovative approaches such as HoneyPot technology have emerged to bolster cybersecurity defenses. This article explores the concept of HoneyPot technology, its benefits, and its role in safeguarding against malicious actors in the ever-evolving digital landscape.

2. Understanding HoneyPot Technology:

HoneyPot[2] technology refers to a cybersecurity technique that involves setting up decoy systems, applications, or networks to attract and deceive malicious actors. These decoy systems, known as HoneyPots, are designed to mimic legitimate targets, enticing cybercriminals to interact with them. While the attackers' attention is focused on the HoneyPot, the actual critical systems and data remain protected and monitored by cybersecurity professionals.

Honeypot technology is a technique used to deceive hackers and deploy honey.The tank system is mainly used to collect network attack intelligence, and traditional defense measures Firewalls and IDS can only prevent known intrusions, while new ones.The invasion of knowledge cannot be prevented and belongs to passive defense. Honeypot technology is just Okay, that's a great addition can actively defend. Honeypot Technology Generally applied in the following three aspects:

(1) To protect real servers. Server, administrators usually deploy the real server on the internal network, and another server with a honeypot system is exposed on the external network. To access a real server, users must first access the honeypot system server. Server, and then link to the real service through the honeypot system server Device, so even hackers cannot directly access the internal network and cannot directly Launch an attack on the real server, thereby affecting the real server the role of protection.

(2) Deploy a server with the same functionality as a real server

The honeypot server intentionally set up some vulnerabilities to lure hackers to actively attack. Attack based on the hacker's intrusion behavior, one can grasp the attack used by the hacker

Tools and intrusion methods, as well as potential innovations in real servers. Vulnerability facilitating reinforcement of real servers to improve authenticity the defense capability of the server.

(3) Hackers who illegally enter the system generally. There will be relevant intrusion records left, and network administrators can use professional .Tool software captures and analyzes intrusion behavior, making it easy for administrators Timely collect intrusion evidence and lure criminals.

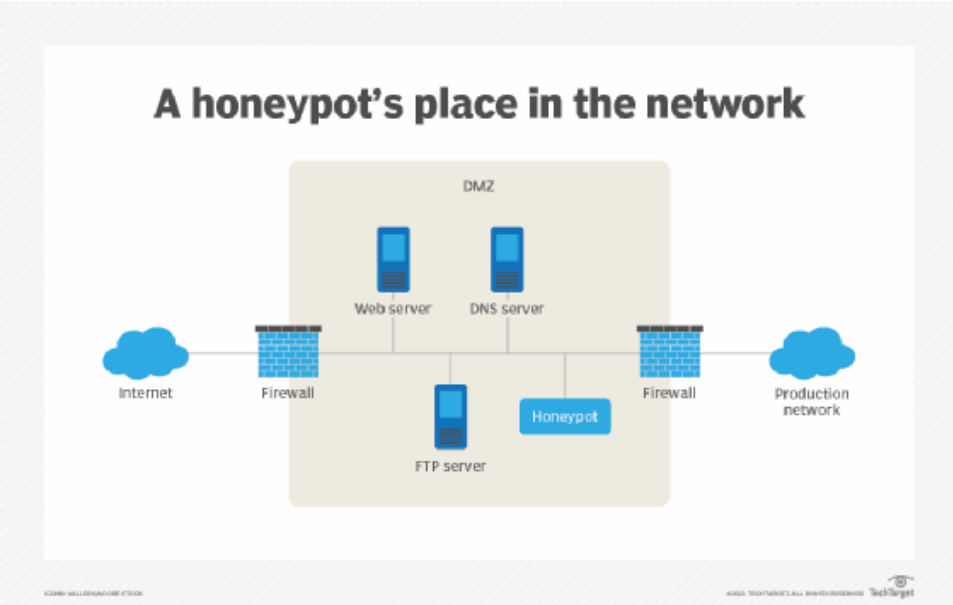

Figure 1. A honeypots are placed at a point in the network.

The Benefits of HoneyPot Technology:

Early Threat Detection: HoneyPots act as an early warning system, providing valuable insights into the tactics, techniques, and procedures employed by attackers. By analyzing their interactions with the decoy systems, cybersecurity experts can identify emerging threats and develop proactive defense strategies.

3. Diversionary Tactics:

HoneyPots divert malicious actors away from genuine assets, reducing the risk of successful attacks on critical systems. As attackers waste their time and resources on the decoy systems, organizations can fortify their actual defenses and respond effectively to potential threats.

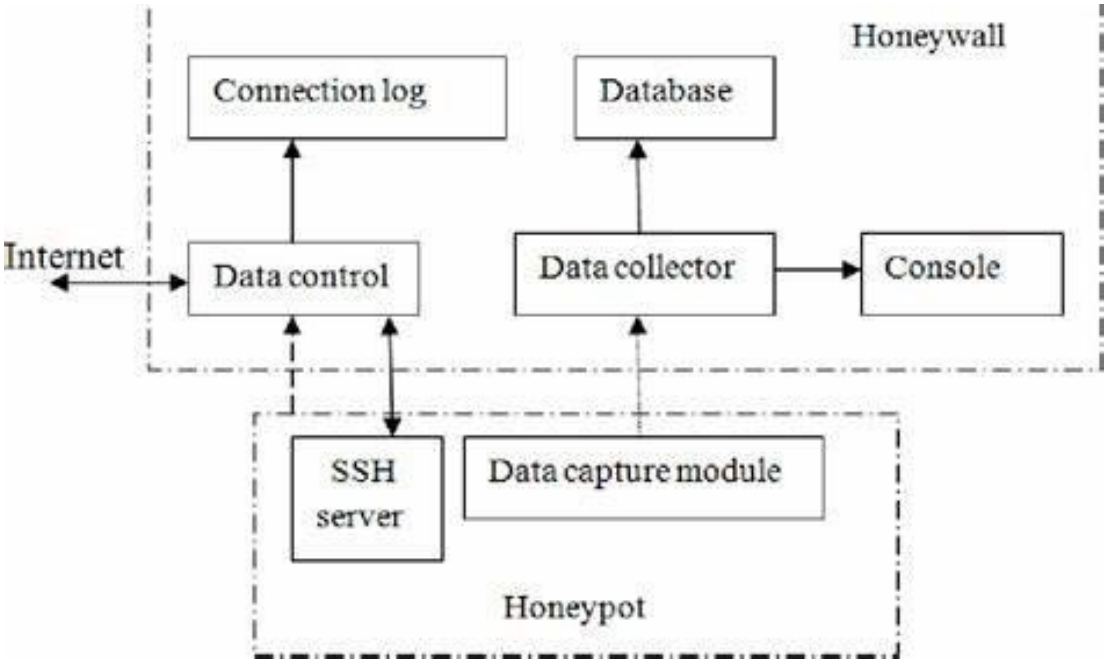

Figure 2. What is a honeypot? How does it secure your SMB?

Gathering Intelligence: HoneyPots serve as a computer simulation tool, enabling organizations to gain a deeper understanding of the motives and capabilities of adversaries. The information collected from HoneyPot interactions helps in enhancing threat intelligence, strengthening incident response procedures, and developing targeted countermeasures.

Vulnerability Analysis: Since HoneyPots are intentionally designed to be attractive targets, any successful interaction with them indicates a potential vulnerability in the network or system. By analyzing the methods used by attackers to breach the decoy systems, organizations can identify and address security weaknesses before they are exploited in real-world attacks.

Legal and Ethical Advantage [3]: When organizations deploy HoneyPots, they have the legal and ethical authority to monitor and collect information about attackers. This data can be used to provide evidence for legal actions, improve law enforcement investigations, and contribute to the broader cybersecurity community's knowledge base.

The "big data" strategy is being extensively discussed in the international community, which is crucial for companies and the process of data sharing and open source in other organizations is also accelerating, and how to effectively maintain the massive network.

Collecting valuable intelligence from network information sources to support the strategic decisions of enterprises is a challenge Difficulties to solve. Previously, individual organizations and businesses mainly relied on manual browsing or search engines. Obtaining network information through manual browsing has strong pertinence and can achieve accurate and effective results. Competitive intelligence, but with a large workload and a wide range of available information. After the advent of the times, search engines can be used to automatically retrieve a large amount of information. Helps to obtain intelligence and even competitive intelligence. But currently, mainstream search engines are popular

The service mode of the core collection service is to retrieve all queries from all users, so the core collection service is also.

It is to collect as much information as possible. This kind of indistinguishable subject and does not cover everything. Answers with light emphasis have had a certain negative impact on intelligence collection, such as reducing. The accuracy and value of intelligence. Answer to information collection on topics in the big data environment. It provides a new way to solve this problem. Theme oriented network intelligence collection. The collection system only accesses the theme of the relevant day on the webpage of the relevant day page, which helps to improve the relationship between the two parties. The daily connection of newspaper collection has narrowed down the scope of page collection and further improved the situation. The speed and effectiveness of report collection. This is just a small application of big data for intelligence collection.

On the basis of the original intelligence collection requirements and themes, after the data is open source, it can be mentioned that. Develop more diverse thematic oriented online competitive intelligence collection systems, while also enabling. Conduct a comprehensive analysis of some key factors that affect the collection of online competitive intelligence.

4. Challenges and Considerations:

While HoneyPot technology offers significant advantages, several challenges and considerations should be kept in mind:

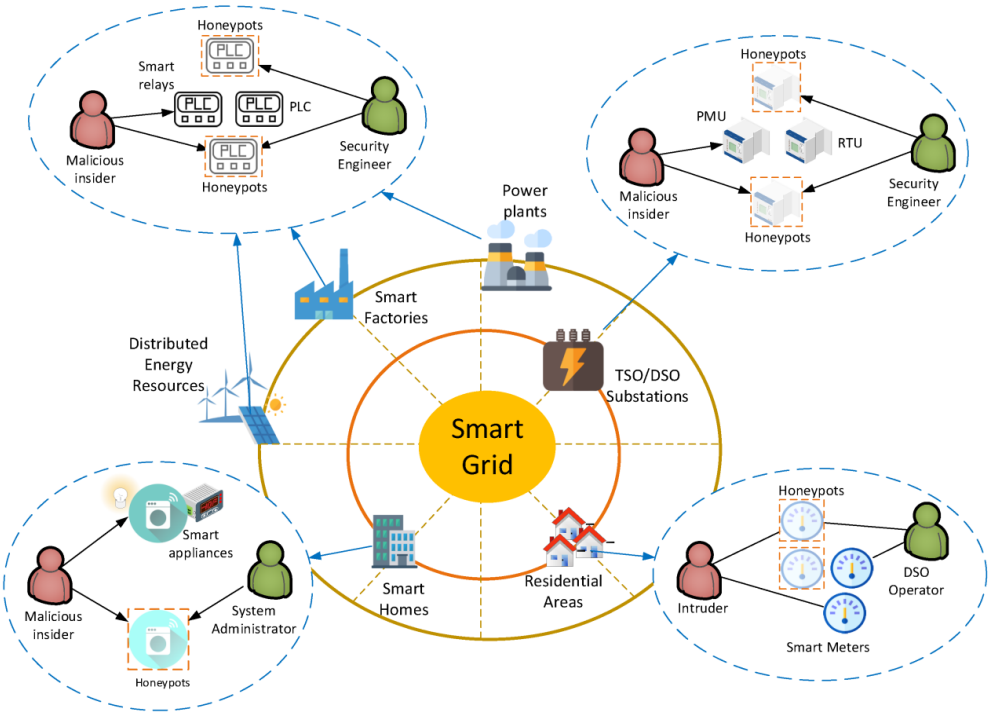

Figure 3. Challenges and Considerations.

Resource Allocation: Setting up and maintaining HoneyPots requires dedicated resources, including hardware, software, and personnel. Organizations need to carefully assess the costs and benefits associated with implementing this technology.

False Positives and Negatives [4]: HoneyPots can sometimes generate false positives (indicating an attack where there is none) or false negatives (failing to detect an actual attack). Regular monitoring and fine-tuning of HoneyPot configurations are necessary to minimize these occurrences.

Security Risks: If not properly isolated and secured, HoneyPots can become entry points for attackers to infiltrate the main network. Robust isolation measures should be implemented to prevent unauthorized access and ensure that HoneyPots do not compromise overall security.

5. Conclusion

HoneyPot technology serves as a valuable addition to the cybersecurity arsenal, providing organizations with an effective means to detect, divert, and gather intelligence on potential threats. By leveraging deception and distraction tactics, HoneyPots enhance the overall security posture and enable proactive defense against cybercriminals. However, organizations must carefully assess the costs, risks, and benefits associated with implementing HoneyPot technology to ensure its successful integration into their cybersecurity strategy [5].

Acknowledgments

This dissertation is supported by 2022 Hunan Province General Higher Education Teaching Reform Research Project (Practical Ability of College Students Based on RBL Model in the Context of Online Education Training Research - Taking the Direction of Network Information Security as an Example. Grant No: HNJG-2022-1016).

References

[1] Mayra M, Chunming W, Walter F. Adversarial examples: A survey of attacks and defenses in deep learning-enabled cybersecurity systems [J]. Expert Systems with Applications, 2024, 238(PE).

[2] D. T O, A. V N, A. D M. Applying Honeypot Technology with Adaptive Behavior to Internet-of-Things Networks [J]. Automatic Control and Computer Sciences, 2022, 55(8).

[3] J. J N. Investor information gathering and the resolution of uncertainty [J]. Journal of Accounting and Economics, 2022, 74(1).

[4] LAN J. Research and Implementation of the Network Honeypot Technology in the Enterprise Network Security - Taking Hospital Enterprises as an Example [J]. BASIC & CLINICAL PHARMACOLOGY & TOXICOLOGY, 2020, 126.

[5] Zhao J, Dong Q L, Yang S M, et al. Research on Technological Innovation of Honeypot [J]. Advanced Materials Research, 2014, 3470(1030-1032).