The application of honey pot technology in network attack and defense of campus network

Zhengchun Zhou * and Wenyao Shen

College of Information Engineering, Shaoyang Campus network, Shaoyang 422000, China

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

Abstract. With the proposal of the thought of Internet power, the domestic cybersecurity emergency drills are more and more frequent. The cybersecurity of campus network is facing increasingly complex and severe threats. Effective means are needed to protect campus network and information system. A honeypot device is a specially designed system or network. It can simulate the real system and high-risk vulnerabilities, in order to attract the attention of attackers, so as to collect attack intelligence, identify vulnerabilities, analyze attack behavior, and further enhance the awareness of cybersecurity in campus network, enhance the ability of cybersecurity emergency response.

Keywords: Cybersecurity; Honeypot; Intrusion detection; Cyber threats.

1. Introduction

With the continuous development and practical application of Internet technology, our country has put forward the idea of network power, and Cybersecurity has become an important part of national security. In the following, I will analyze the importance of honey pot technology in campus network through five chapters: the overview of the honey tank equipment, the design and implementation of the honey pot equipment, the application of the honey pot equipment in Cybersecurity, the advantages and challenges of the honey pot equipment, and the future development of the honey pot equipment.

2. Application of honey pot

2.1. Invasion detection

Honey pot equipment plays an important role in detecting and preventing intrusion, especially in attack detection and monitoring, collecting attack data, learning attacker strategies, detecting zero-day vulnerabilities, alerts and response, risk reduction, threat intelligence and analysis [1].

In short, honeypot equipment plays a key role in detecting and preventing invasion, by simulating vulnerable targets, attracting attackers, monitoring attacks, providing attack data, and generating threat intelligence, thus helping to improve the level of Cybersecurity and early detection and response to potential threats. As shown in Figure 1:

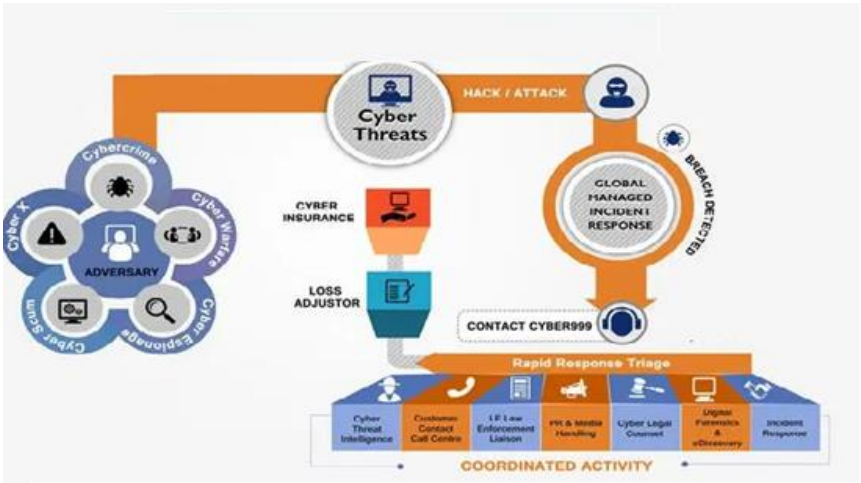

Figure 1. Invasion detection and evidence collection.

2.2. Threat intelligence

Using honey pot equipment to collect threat intelligence is one of the important means to improve security defense [2]. Threat intelligence provides critical information about current threats and attacker behavior, helping organizations take appropriate measures to mitigate risks and improve cybersecurity defenses. So how do you use honeypot equipment to collect threat intelligence? We currently have the following methods:

Improve defense strategies: Use collected threat intelligence to improve cyber defense strategies and adjust security policies, rules, and configurations to better respond to known threats.

Real-time response: Use threat intelligence to respond to new attacks in real time, such as blocking an attacker's IP address or fixing known vulnerabilities.

Honeypot equipment can be used not only to detect intrusion, but also to actively gather information about attackers and threats. This intelligence is critical to improving cybersecurity strategies, risk mitigation, and improving response capabilities. As shown in Figure 4:

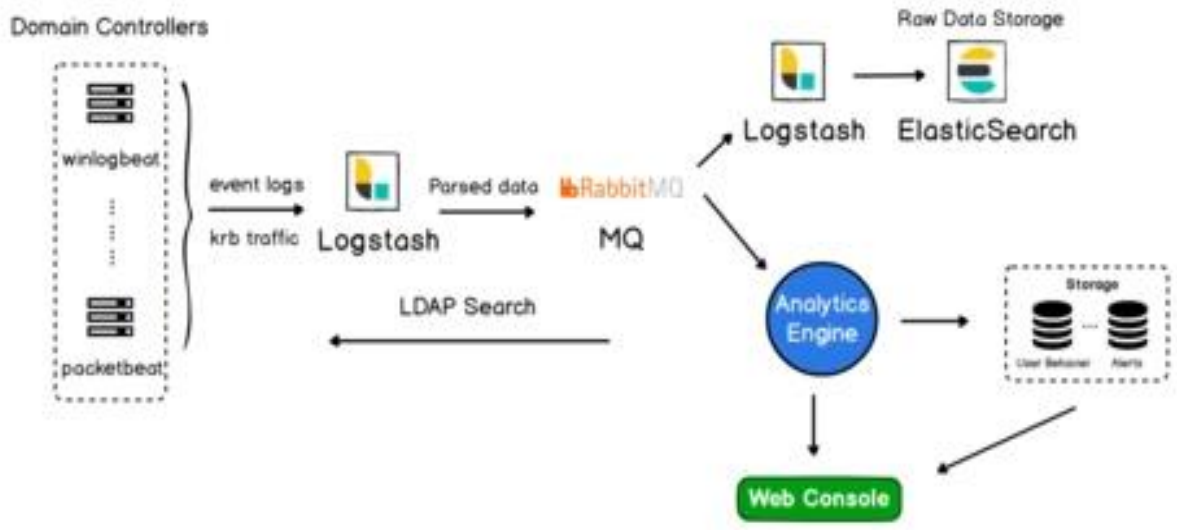

Figure 2. Honey pot intelligence collection.

2.3. Attsor behavior studies

By analyzing the honeypot equipment data, you can gain insight into the attacker's behavior and strategies to provide valuable threat intelligence and Cybersecurity insights. Analyzing honeypot equipment data to gain insight into attacker behavior and strategy in the following ways:

Malicious command and control communications: Analyze the communication between attackers and the honeypot to learn whether they try to establish backdoors, manipulate honeypot devices, or transmit malicious commands [3].

Attacker strategy adaptability: observe whether the attacker adjusts their strategy according to the changes in the network environment. This can help the security team to predict the possible actions of the attacker.

By comprehensive analysis of the honeypot equipment data, the security team can gain a deep understanding of the attacker's behavior and strategy. This helps to improve cybersecurity strategies, strengthen defmeasures, and provide valuable insights into potential threats. See Figure 5 below for the attacker traceability analysis:

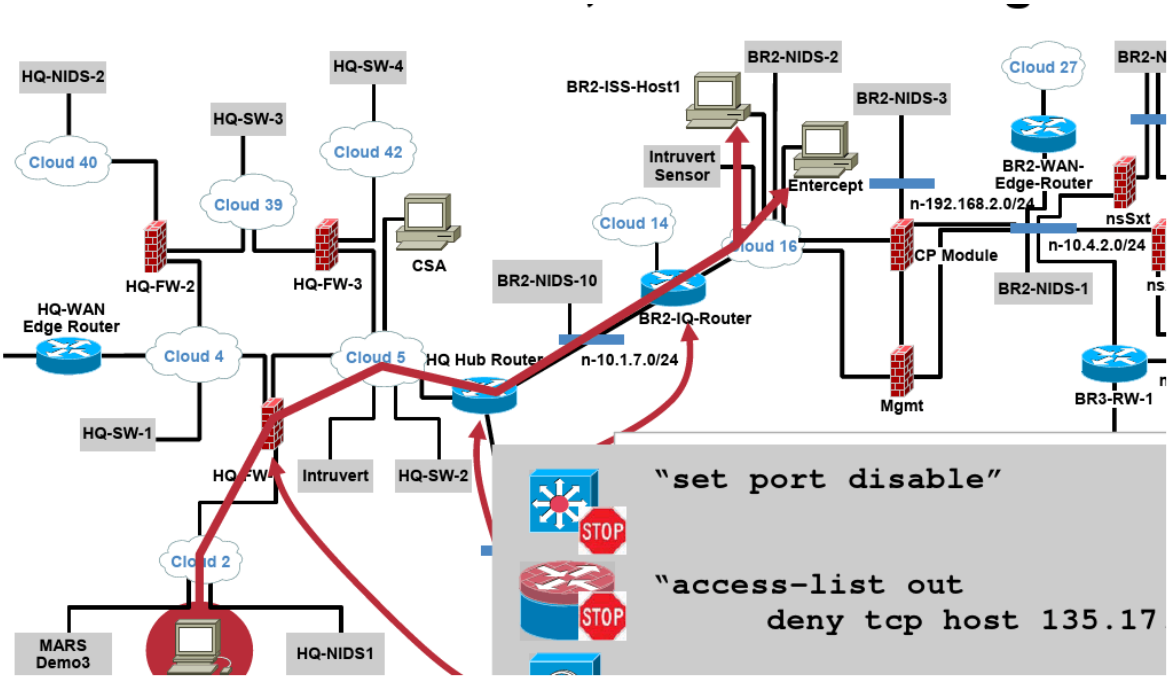

Figure 2. Attack traceability scene.

3. Advantages and challenges

Honey pot equipment has some significant advantages over other security measures, including active threat detection, attack intelligence collection, inducing attackers to distract themselves, zero-day vulnerability detection, security education and training, in-depth analysis and simulation, custom configuration, and low false alarm rate.

Despite these advantages, honeypot devices also need to be used with caution as they require additional resources and management to ensure their efficacy and safety. The best cybersecurity strategy is usually a combination of multiple security measures, including honeypot equipment, to provide comprehensive protection.

4. Future development of honeypot equipment

Containerization and microservices: deploying honey pots using container and microservice technologies to improve flexibility and scalability. These technologies allow honeypots to be rapidly deployed and reorganized to accommodate diverse network environments.

Analysis of attacker behavior: Analysis based on attacker behavior is an important trend in honeypot technology. Analysis of the attacker's behavior patterns provides a better understanding of the attack strategies and targets [4].

Compliance and Compliance: As regulatory requirements for data privacy and security increase, compliance and compliance with honeypot equipment become more important. Honeypot technology needs to be consistent with relevant regulations to prevent potential legal issues [5].

In short, the field of honey pot technology is constantly evolving to adapt to new threats and challenges. The future direction will continue to focus on technology trends in intelligence, automation, cloud, and threat intelligence integration and attacker behavior analysis.

5. Conclusion

Honeypot equipment has a wide range of potential applications, covering Cybersecurity, threat intelligence, research and training. At present, in addition to the above-mentioned application scenarios, I think the honey pot can also cover many fields, such as police forensics, vulnerability

research, malware research, and so on. In the continuous evolution of Cybersecurity, honey pot equipment, as an important security tool, will continue to contribute to the protection of the network and improve security awareness [6].

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] Snow Qing. Research on network intrusion detection technology based on honeypot [D]. Changchun Campus network of Technology, 2023.DOI:10.27805/d.cnki.gccgy.2023.000785.

[2] Zhang Kezhu. Analysis and research on network attack behavior based on honeypot technology [J]. Journal of Yellow River Institute of Science and Technology, 2022, 24(11):45-48.DOI:10.19576/j.issn.2096-790X.2022.11.009.

[3] Liu Yonghui, Hu Qiaojie, Zhao Li. Design of LAN security defense system based on honeypot technology [J]. The Electronic Design Engineering, 2022, 30(14):68-72.DOI:10.14022/j.issn1674-6236.2022.14.015.

[4] Su Xiang. Research on the application of honeypot technology in enterprise Cybersecurity protection [J]. Information and Computer (theoretical edition), 2022, 34 (07): 35-38.

[5] And Deli Lau. Analysis of network attack traceability technology based on honeypot trap [J]. Confidential Science and Technology, 2022 (01): 31-36.

[6] Zhao Jinmeng, Zhang Jing, Su Beibei and so on. Design of enterprise network hacker intrusion defense system based on honeypot technology [J]. Enterprise Technology and Development, 2022 (01): 50-52.