RESEARCH ARTICLE | FEBRUARY 05 2025

Honeypot-based IDS for cyber attack detection

M. Karthigha; M. Indira Priyadharshini ✉; M. Rohini; J. Reema Nafeesa; B. ShreeAkshaya; R. Yagavi

AIP Conf. Proc. 3204, 040018 (2025)
https://doi.org/10.1063/5.0245939

Honeypot-based IDS for Cyber Attack Detection

M Karthigha[1, a)], M Indira Priyadharshini[2, b)], M Rohini[3, c)], J Reema Nafeesa[2, d)], B ShreeAkshaya[2, e)] and R Yagavi[2, f)]

[1]*Department of Computer Science and Engineering, PSG Institute of Technology and Applied Research, Coimbatore, India.*
[2]*Department of Computer Science and Engineering, Sri Ramakrishna Engineering College, Coimbatore, India.*
[3]*Department of Computer Science and Engineering, Sri Krishna College of Engineering and Technology, Coimbatore, India.*

[a)] karthighamohan@gmail.com
[b)] Corresponding author: indirapriyadharshini.m@srec.ac.in
[c)] rohinim@skcet.ac.in
[d)] reemanafeesa.2101212@srec.ac.in
[e)] shreeakshaya.2101230@srec.ac.in
[f)] yagavi.2101258@srec.ac.in

Abstract. As technology elaborates daily, maintaining enormous amounts of data has become a great challenge. Security becomes vulnerable starting from zero-day attacks to malware threats. It is necessary to bring a solution to this without compromising data integrity and data security. This calls for an intrusion detection system that can detect suspicious activities while alerting the users. Honeypots are one such system that enables us to carry out the same. It is a type of network security system that is becoming increasingly popular in modern network architecture due to its ability to detect malicious activities from external sources. Honeypots simulate a high-value target and lure potential attackers away from critical systems. Thus, a honeypot, in simple words, is a fake system that acts as trap alluring intruders to seek the system/data. It entices the users to perform attacks instead where information about attacks is recorded. The honeypot creates a decoy environment to divert intruders to detect, track, deter, and prevent unauthorized access to the network. As evidenced by its growing popularity in security, the honeypot is an invaluable addition to a comprehensive security plan. The project proposes a honeypot system that imitates a telnet port. This telnet port works by deceiving attackers and retrieving information about them.

INTRODUCTION

Conventional methods of security are not effective when data size grows. These methods do not provide solutions for all security concerns. Traditional methods like signature-based IDS provides limited coverage and many false negatives. These systems may not be effective at detecting certain types of attacks. failure is inevitable so, It is a challenge to handle important details on a large scale. A honeypot is such a security mechanism that can detect and study unauthorized use of information. A honeypot is an endeavor aimed at creating a decoy system that mimics the behavior of real systems to attract potential attackers and detect their actions. They are computer networks that are intentionally enticing to potential attackers. They are nothing but traps set up by security professionals to lure in attackers and gather information about their tactics, techniques, and procedures (TTPs).

Honeypots provide a way to minimize vulnerability and provide security against any kind of intrusion. The main purpose of the honeypot is to create a secure environment for monitoring and detecting malicious activity on a network. It showcases itself to be a legitimate target for attackers while in reality, it is a trap set up by security experts to gather information about the attacker and alert the main system. They are much more convenient compared to other security mechanisms. The project works by listening to the open port for attackers and detecting suspicious activities. When attackers try to intrude through the open ports the honeypot works effectively by detecting the attack and alerting

International Conference on Innovations in Robotics, Intelligent Automation and Control (ICIRIAC2024)
AIP Conf. Proc. 3204, 040018-1–040018-5; https://doi.org/10.1063/5.0245939
Published under an exclusive license by AIP Publishing. 978-0-7354-5114-8/$30.00

In Figure 2, when a remote host searches for the open port in the system, the port 21 where the honeypot is deployed is portrayed as an open port. This is responsible for alerting the system about potential attacks along with the log information. In Figure 3, a fake banner is displayed when an attacker gets into the port which is the honeypot. It makes the attacker think that he has successfully broken into the system while echoing the information about the attacker simultaneously.

CONCLUSION AND FUTURE ENHANCEMENTS

In today's technology, with everything requiring the internet, security is highly compromised. Attacks, breaches, data thefts, and intrusions have become inevitable. Honeypots deliver an efficacious solution to these disputes. They can be regarded as a key tool to watch over corporate and individual attacks that may occur to a user or to an organization.

The project calls for zero investment. It requires less time and maintenance when compared to other alternatives. It does not require large complex resources to deploy in the system. It detects any intrusion at the earliest stage itself and provides security to the main system.

In the future, the data about the attacks detected by the honeypot shall be analyzed. In addition to this, an intelligent honeypot that differentiates benign and dangerous attacks based on signatures will be developed.

REFERENCES

1. Aaditya Jain and Bala Buksh, International Journal of Engineering Trends and Technology **29**, 304-312 (2015).
2. I. Kuwatly, M. Sraj, Z. Al Masri and H. Artail, "A dynamic honeypot design for intrusion detection," The IEEE/ACS International Conference onPervasive Services, in *ICPS 2004. Proceedings*., Beirut, Lebanon, 2004, pp. 95-104.
3. Abhishek Mairh, Debabrat Barik, Kanchan Verma and Debasish Jena, "Honeypot in network security: a survey," in *ICCCS '11: Proceedings of the 2011 International Conference on Communication, Computing & Security*, 2011, pp. 600-605.
4. Neha Titarmare, Nayankumar Hargule and Anand Gupta, International Journal of Computer Sciences and Engineering **7**, 394-397 (2019).
5. E. Balas and C. Viecco, "Towards a third generation data capture architecture for honeynets," in *Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop*, West Point, NY, USA, 2005, pp. 21-28.
6. X. Meng, Z. Zhao, R. Li and H. Zhang, "An intelligent honeynet architecture based on software defined security," in *9th International Conference on Wireless Communications and Signal Processing (WCSP)*, Nanjing, China, 2017, pp. 1-6.
7. C.Y. Wang, Y.L. Jhao, C.S. Wang, S.J. Chen, F.H. Hsu and Y.H. Chen, "The bilateral communication-based dynamic extensible honeypot," in *International Carnahan Conference on Security Technology (ICCST)*, Taipei, Taiwan, 2015, pp. 263-268.
8. Ci-Bin Jiang, I-Hsien Liu, Yao-Nien Chung and Jung-Shian Li, International Journal of Network Management **26**, 156-175 (2016).
9. Kumar Shridhar and Mayank Jain, International Journal of Science and Research **3**, 1038-1043 (2014).
10. Selvakumar Veluchamy and Ruba Soundar Kathavarayan, International Journal of Intelligent Systems **37**, 3981-4007 (2022).