EIU
Emirates International University Journal
مجلة الجامعة الإماراتية الدولية

Volume 1 Issue 1
23-8-2025

Honeypots Technology in Combat Cybercrimes

Dr. Malek Algabri [1,1]
Ph.D. in Computer Science and Technology
dr.malekye@eiu.edu.ye

Dr. Gamil R. S. Qaid [2,2]
Ph.D. in Computer Sciences and Engineering
dr.gamil@eiu.edu.ye
dr.g_qaid@hoduniv.net.ye

Ehab Waleed Al-Junid [3,3*]
Senior Student, B.Sc. in Information Security
ehabw898@gmail.com

Department of Cybersecurity, Faculty of Engineering and Information Technology,
Emirates International University, Sana'a, Yemen

Abstract

This study presents a practical cybersecurity framework using honeypot technology to detect and analyze cyber threats. By deploying simulated systems such as Cowrie, Amun, and Wordpot within a virtualized environment using VMware and GNS3, the research demonstrates how deception can effectively engage attackers and capture their behavior. The system is integrated with the Modern Honey Network (MHN) for centralized monitoring and log collection. Simulated attacks including SSH brute-force and web probing were carried out using Kali Linux and analyzed with Wireshark. The results show that honeypots provide valuable threat intelligence, enhance detection capabilities, and support proactive defense strategies in a secure and isolated environment.

Keywords: Honeypot; Cowrie; SSH; Cybersecurity; Network Emulation;

1. Introduction

In today's digital era, cybersecurity has become a top priority due to the rapid evolution and increasing frequency of cyber threats. According to recent global statistics, a cyber-attack occurs approximately every 39 seconds, threatening the security and continuity of digital infrastructures. Traditional defense mechanisms, such as firewalls and intrusion detection systems (IDS), are often limited in detecting unknown or advanced attacks, especially those exploiting zero-day vulnerabilities or bypassing signature-based detection.

Honeypot technology has emerged as an effective countermeasure, offering a proactive and deceptive approach to network security. By deploying decoy systems that mimic real services, honeypots lure attackers into interacting with fake environments, allowing security professionals to study their behavior without endangering real assets. This study proposes a multi-layered honeypot framework utilizing Cowrie, Amun, and Wordpot honeypots within a fully virtualized environment. The goal is to detect, analyze, and respond to cyber threats in real-time, thereby enhancing threat intelligence and supporting resilient defense strategies.

2. Related Work and Framework Comparison

Several studies have investigated the role of honeypots in cyber threat detection and analysis. For instance, Steingartner et al. developed a cyber deception model utilizing honeypots to improve resilience against hybrid threats. Similarly, Yang et al. introduced a high-interaction honeypot framework for proactive threat management. Other researchers, including Mohtasin and Raghul, have explored the integration of virtual environments such as VMware and GNS3 for honeypot deployment.

However, many existing approaches either focus on a single honeypot type or lack centralized monitoring and traffic analysis. This study differs by implementing a modular framework that integrates multiple honeypots

(Cowrie, Amun, and Wordpot) managed via the Modern Honey Network (MHN) within a fully simulated and segmented virtual environment. This enables comprehensive monitoring, realistic attacker engagement, and efficient forensic analysis, bridging the gap between theoretical research and practical implementation.

3. Contribution

This research provides a practical and scalable honeypot-based framework for cyber threat detection, analysis, and mitigation. Unlike traditional systems that primarily rely on prevention, this approach uses deception to actively interact with attackers. The main contributions are:

- **Multi-honeypot architecture**: Combines Cowrie (SSH), Amun (low-interaction), and Wordpot (CMS) honeypots to simulate diverse attack surfaces.
- **Virtualized isolated environment**: A secure network built with VMware and GNS3 ensures safe experimentation.
- **Integration with MHN**: Enables centralized logging, monitoring, and attack visualization.
- **Realistic attack simulation**: Uses Nmap, Kali Linux, and Wireshark for comprehensive analysis.
- **Threat intelligence generation**: Collects and analyzes attacker behavior for improved defense strategies and awareness.

4. Problem Statement

Traditional cybersecurity systems face significant limitations in detecting sophisticated, unknown, or zero-day attacks. Most rely heavily on predefined rules, known signatures, or anomaly detection, which makes them vulnerable to new or adaptive attack strategies. In addition, these systems often generate high volumes of false alerts, overwhelming security teams and reducing the efficiency of response mechanisms.

Furthermore, there is a lack of effective tools for understanding attacker behavior, as traditional defenses focus on prevention rather than engagement. Without interaction with threat actors, it becomes difficult to gather intelligence on their tactics, motivations, and tools. The absence of deception or diversion strategies also allows attackers to target real assets directly.

These challenges highlight the need for a proactive solution that not only detects threats but also interacts with them in a controlled environment. Honeypots offer such a solution by attracting attackers, logging their activities, and supporting detailed analysis, all without risking production systems.

5. Research Objectives

The main objective of this research is to design, implement, and evaluate an effective cybersecurity framework based on honeypot technology to improve threat detection and analysis. The study aims to achieve the following specific objectives:

- To develop a multi-layered honeypot system simulating various services such as SSH, HTTP, and CMS platforms.
- To deploy the system within a segmented and isolated virtual network using VMware and GNS3.
- To collect attacker behavior data using centralized logging (via MHN) and network analysis tools (e.g., Wireshark).
- To analyze the effectiveness of different honeypot interaction levels (low, medium, high) in capturing threat intelligence.
- To demonstrate how honeypots can support real-time monitoring, enhance cybersecurity awareness, and serve as educational and research tools.

6. Research Methodology

This project adopts the Agile methodology as the core development model due to its flexibility, adaptability, and iterative nature. Agile supports incremental development and continuous feedback, making it ideal for dynamic cybersecurity projects that require frequent updates and testing.
The development process was divided into small, manageable tasks such as honeypot installation, network configuration, logging setup, and attack simulation. Each stage was tested and improved based on results and observed performance.
Key tools used include:

- **VMware Workstation Pro**: For hosting virtual machines representing honeypots, attackers, and monitoring systems.
- **GNS3**: For simulating a realistic network environment with DMZ zones and routing.
- **Modern Honey Network (MHN)**: For centralized honeypot management and logging.
- **Kali Linux & Nmap**: To simulate realistic cyber-attacks and reconnaissance.
- **Wireshark**: For detailed packet-level traffic analysis.

The Agile approach ensured continuous refinement, improved collaboration, and timely identification of potential issues during implementation.

7. Scenario and Simulation

To assess the effectiveness of the proposed honeypot framework, a simulated environment was built using VMware Workstation Pro and GNS3. This virtual network includes segmented zones with multiple honeypot systems, an attacker machine, and monitoring components.

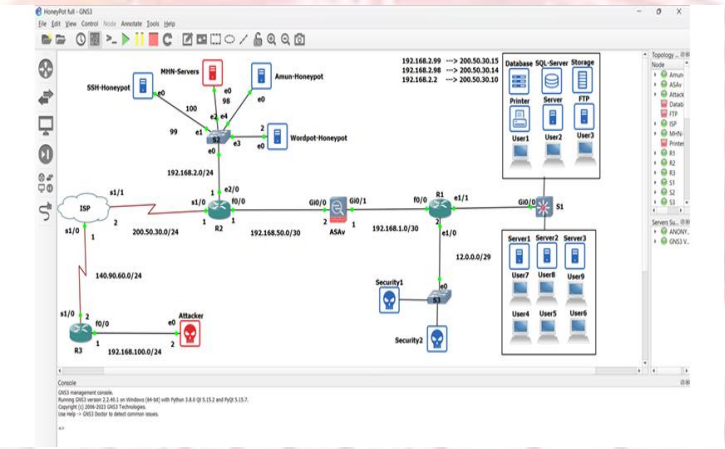

Fig. 1 Network architecture of the honeypot environment designed in GNS3.

The deployed honeypots include:

- **Cowrie** (High-Interaction SSH Honeypot)
- **Amun** (Low-Interaction Generic Service Honeypot)
- **Wordpot** (Web-based CMS Honeypot for WordPress)

These systems are centrally managed through the Modern Honey Network (MHN), which collects logs and visualizes attack patterns.
The attacker machine runs Kali Linux and performs various reconnaissance and attack techniques using tools

such as Nmap and Hydra. Scenarios include:

- SSH brute-force attacks on Cowrie
- Telnet and HTTP probing of Amun
- WordPress login and plugin enumeration attempts on Wordpot

All network activity is monitored and analyzed using Wireshark to inspect traffic and confirm attacker interaction with the honeypots.

8. Challenges

During the development and testing of the honeypot-based framework, several challenges were encountered:

1. **Balancing realism and safety**: Creating believable honeypot environments without exposing the internal network required careful isolation.
2. **Complex network configuration**: Integrating honeypots with GNS3 and VMware while configuring VLANs, firewalls, and routing policies was technically demanding.
3. **Hardware limitations**: Running multiple virtual machines and monitoring tools consumed significant system resources.
4. **False positives**: Low-interaction honeypots occasionally produced misleading alerts due to generic probes.
5. **Data overload**: Consolidating logs from Cowrie, Amun, Wordpot, MHN, and Wireshark led to large volumes of data requiring effective filtering and correlation.
6. **Maintenance effort**: Regular monitoring, script updates, and system resets were needed to maintain functionality and realism.

Addressing these issues was essential for achieving reliable, secure, and scalable honeypot deployment.

9. Results

The deployment of the honeypot framework produced promising outcomes in terms of threat visibility and system functionality. Key findings include:

- Successful system deployment: A fully operational environment was established with MHN managing all honeypots.

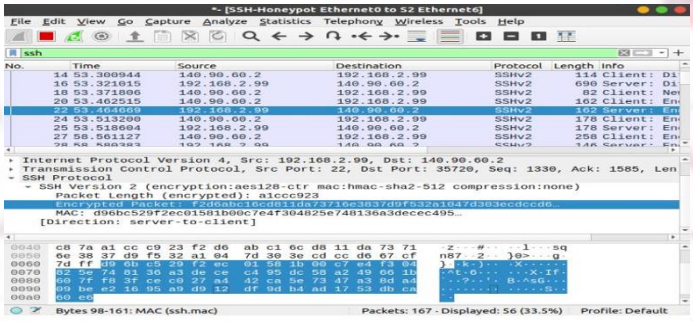

Fig. 2 Wireshark analysis of SSH brute-force attack traffic.

- Realistic attacker interaction: Simulated attacks were effectively captured, including brute-force attempts, service scans, and CMS exploitation probes.
- Detailed behavioral logs: Cowrie captured shell commands, login attempts, and file manipulations; Wordpot detected WordPress-specific scans; Amun logged service probes.
- Traffic analysis with Wireshark: Provided packet-level insight into the methods and tools used by

attackers.

- Visualization and statistics: MHN dashboards presented real-time metrics on attack frequency, top targets, and source IPs.

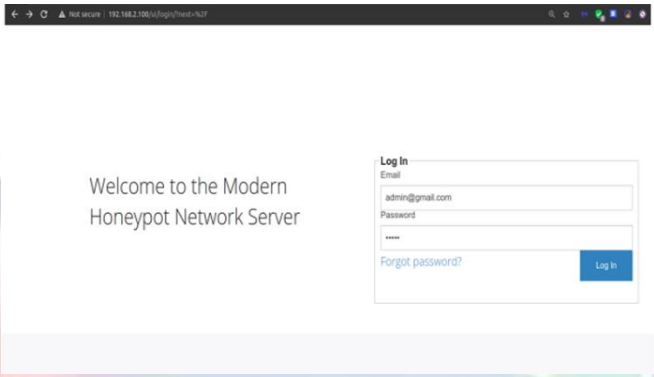

Fig. 3 shows the server settings MHN.

- Security assurance: Despite simulated breaches, internal systems remained protected due to proper segmentation and firewall policies.

10. Authors' Biographies

Dr.Malek_Nasser_Ali_Algabri
(*dr.malekye@eiu.edu.ye*)
Dr. Malek Algabri is an Associate Professor of Cybersecurity at the Faculty of Engineering, Emirates International University, Yemen. He received his B.Sc., M.Sc., and Ph.D. degrees in Computer Science and Technology from Wuhan University of Technology, Wuhan, China, in 2008, 2010, and 2013 respectively. His research interests include Cybersecurity, Artificial Intelligence, Computer Science, and Computer Networks.

Dr.Gamil_R._S._Qaid
(*dr.gamil@eiu.edu.ye*,*dr.g_qaid@hoduniv.net.ye*)
Dr. Gamil Qaid is the Head of the Cybersecurity Department at the Faculty of Engineering and Information Technology, Emirates International University, Yemen. He also serves as an Associate Professor in the Computer Engineering Department at the Faculty of Computer Sciences and Engineering, Hodeidah University, Yemen. He earned his B.Sc. and M.Sc. degrees in Techniques and Technology (Information Technology and Computer Engineering) from Kursk State Technical University, Russia, in 2005 and 2007 respectively. He obtained his Ph.D. in Computer Sciences and Engineering from SGGS College of Engineering and Technology, SRTMU, India, in 2016, with a dissertation titled *"Encryption and Decryption of Images Using Multi-Objective Soft_Computing_Algorithms."*
Dr. Qaid is a member of the Council of Young Scientists of India and a lifelong member of the International Association of Engineers (IAENG). He actively reviews for several international journals and conferences. His research interests include Information Security, Artificial Intelligence, Image Processing, and Cloud Computing. He has published numerous papers in peer-reviewed journals and international conferences.

11. Conclusion

This study demonstrates the effectiveness of honeypot technology in combating cybercrimes through deception and threat intelligence. By integrating multiple honeypots within a virtualized and isolated environment, and managing them via a centralized platform (MHN), the framework successfully captured and analyzed various attack behaviors.

The findings highlight the value of honeypots in supplementing traditional security tools, enhancing detection capabilities, and enabling proactive defense strategies. Furthermore, the system serves as a powerful educational and research tool for studying real-world attack techniques in a safe and controlled manner.

Future work may include automating data correlation, expanding the range of honeypots, and integrating machine learning models to improve anomaly detection and attack classification.

References

[1] University of Maryland. (2017). Hacking Statistics: A cyber-attack occurs every 39 seconds. https://eng.umd.edu/news/story/study-cyberattacks-happen-on-average-every-39-seconds

[2] Steingartner, W., Galinec, D., & Kozina, A. (2021). *Threat defense: Cyber deception approach and education for resilience in hybrid threats model*. Symmetry, 13(4), 597. https://doi.org/10.3390/sym13040597

[3] Steingartner, W., Galinec, D., & Kozina, A. (2021). *Threat defense: Cyber deception approach and education for resilience in hybrid threats model*. Symmetry, 13(4), 597. https://doi.org/10.3390/sym13040597

[4] Mohtasin, R., Prasad, P. W. C., Alsadoon, A., Zajko, G., Elchouemi, A., & Singh, A. K. (2016, March). *Development of a virtualized networking lab using GNS3 and VMware workstation*. In *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)* (pp. 603–609). IEEE. https://doi.org/10.1109/WiSPNET.2016.7566232

[5] Rafique, U. (2021). *Cloud-based Research Honeypots: Technical Report* [Master's Thesis, National College of Ireland]. https://norma.ncirl.ie/5132/

[6] Morić, Z., Dakić, V., & Regvart, D. (2025). *Advancing Cybersecurity with Honeypots and Deception Strategies*. Informatics, 12(1). MDPI AG. https://doi.org/10.3390/informatics12010001

[7] Soepeno, R. A. A. P. (2023). *Wireshark: An Effective Tool for Network Analysis*. CYBV – Introduction to Methods of Network Analysis. https://www.researchgate.net/publication/374978430

[8] Yang, X., Zhang, M., Li, Y., & Wang, Q. (2023). *A highly interactive honeypot-based approach to network threat management*. Future Internet, 15(4), 127. https://doi.org/10.3390/fi15040127

[9] Raghul, S. A., Kalimuthu, R., & Kumaran, S. (2024). *Enhancing cybersecurity resilience: Integrating IDS with advanced honeypot environments for proactive threat detection*. In *2024 3rd International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*. IEEE. https://doi.org/10.1109/ICAAIC60187.2024.10327178

[10] Tetteh, S. G. (2024). *Empirical Study of Agile Software Development Methodologies: A Comparative Analysis*. Asian Journal of Research in Computer Science, 17(5), 30–42. https://doi.org/10.9734/ajrcos/2024/v17i5320