UDC 004.056

D. O. Nemyrovska

THE ROLE OF HONEYPOT SYSTEMS IN MODERN CYBERSECURITY

Vinnytsia National Technical University

Abstract

This paper examines the practical role of honeypot systems in modern cybersecurity. It discusses their core advantages, their evolution toward cloud-native and high-interaction architectures, and the privacy implications of their deployment.

Keywords: honeypot, threat intelligence, cloud-native security, data privacy.

Анотація

У роботі розглядається практична роль honeypot-систем у сучасній кібербезпеці. Розглянуто їхні основні переваги, еволюцію в напрямку хмарних та високоінтерактивних архітектур, а також питання конфіденційності, пов'язані з їх розгортанням.

Ключові слова: honeypot, розвідка загроз, хмарна безпека, конфіденційність даних.

Introduction

Traditional defensive tools like firewalls and intrusion detection systems remain essential, but they share a fundamental weakness: they are reactive rather than proactive. They can only react to threats after they appear, and they struggle to keep up with the speed at which new attack methods emerge [1]. This creates a serious asymmetry between attackers and defenders in cyberspace.

Honeypot technology offers a way to shift that balance. A honeypot is a deliberately crafted trap – a system or resource placed in a network with the purpose of being attacked [1, 2]. It has no legitimate users and no production function. Any interaction with it is, by definition, unauthorized. This makes honeypots exceptionally efficient at separating real threats from background noise: their false detection rate is close to zero [2]. The data they capture – attacker tools, tactics, and objectives – can then be analyzed to better understand vulnerabilities and strengthen defenses for the actual network environment [1].

Core Advantages

The most frequently cited advantage of honeypots is their low false-positive rate. Since no legitimate user should ever interact with a honeypot, virtually every recorded event represents actual malicious activity [2]. This is a significant improvement over traditional IDS sensors, which generate large volumes of alerts that security teams must manually filter.

Honeypots also excel at detecting unknown threats. Signature-based tools can only identify attacks they have been programmed to recognize. A honeypot does not rely on signatures – it captures whatever is directed at it, including zero-day exploits and novel techniques [2]. The European Union Agency for Cybersecurity has identified ransomware, malware, and zero-day exploits as the primary cyber threats in its recent reports, and automated scanners have been documented finding vulnerable devices within 15 minutes of a vulnerability disclosure [3]. In this environment, tools that can detect the unexpected – rather than only the known – are essential.

Beyond detection, honeypots serve as research instruments. They collect in-depth information about attacker behavior that few other technologies can match. This includes the commands attackers execute, the credentials they attempt, the tools they upload, and the communication patterns they use [1, 4].

Cloud-Native and High-Interaction Systems

Honeypot technology has evolved considerably. Early honeypots were simple Linux installations placed on spare hardware. Today, they are deployed as lightweight, containerized cloud resources that can simulate a wide variety of services and devices [3].

Yang et al. demonstrate a modern high-interaction honeypot architecture that uses a modular design with a central management node [1]. Their system separates the honeypot environment from the data processing node, making it easier to add, remove, or modify honeypots without complex reconfiguration. High-

interaction honeypots provide real operating systems and services rather than simple emulations, which allows them to capture far more detailed information about attacker behavior – including new rootkits, lateral movement techniques, and post-exploitation activity [1].

Priya and Chakkaravarthy take this further with a containerized, cloud-based honeypot architecture [4]. Their system deploys an ensemble of honeypot detectors using container technology, which makes scaling practical and cost-effective. The researchers emphasize that discovering malicious packets among normal cloud activity using only IDS or log analysis is challenging and time-consuming. Honeypots address this by providing a clean signal: since they simulate real systems but have no legitimate traffic, any activity they capture is inherently suspicious [4].

Real-World Threat Data

Honeypots are not theoretical tools – they produce concrete, actionable intelligence. A 2023 study by Outpost24 deployed 20 honeypots distributed globally and registered 42 million attacks between January and September 2022 [5]. Brute-force attacks were the most common type, with default credentials attempted over 5.5 million times. Ports 445 and 22 – corresponding to Windows file sharing and SSH remote access services – were the most targeted [5].

This kind of data has direct practical value. It reveals which services attackers target most, which credentials they try first, and which regions generate the most scanning activity. Organizations can use these findings to prioritize patching, adjust firewall rules, and harden their most exposed services.

Privacy Considerations

Deploying honeypots raises legal questions, particularly in jurisdictions with strong data protection frameworks. Honeypots inevitably collect information about attackers, including IP addresses. Under EU law, IP addresses are classified as personal data [6]. This means that honeypot operators must consider how data is collected, how long it is retained, and whether it can be shared.

Sokol, Míšek, and Husák provide a detailed analysis of these issues [6]. They point out that the legal framework influences not only what data honeypots may collect, but also what operators can do with that data afterward. When researchers wish to publish honeypot findings, anonymization is necessary [6]. The authors emphasize that while the cybersecurity value of honeypots is clear, responsible deployment requires awareness of the applicable legal constraints.

Conclusion

Honeypot systems have grown from simple experimental setups into mature, scalable components of modern cybersecurity infrastructure. They provide high-quality threat data with near-zero false positives, detect attacks that signature-based tools miss, and generate intelligence that directly informs defensive decisions [1, 2]. Modern deployments leverage containerization, cloud platforms, and modular architectures to make honeypots practical for organizations of various sizes [1, 3, 4]. Real-world data from large-scale honeypot networks – such as the 42 million attacks captured by Outpost24 in 2022 – demonstrates their operational value [5].

At the same time, privacy and legal compliance remain important considerations, particularly in the European Union [6]. As cyber threats continue to evolve, honeypot technology is evolving alongside them – shifting cybersecurity from purely reactive defense toward active intelligence gathering

REFERENCES

1. Yang, X. A Highly Interactive Honeypot-Based Approach to Network Threat Management [Text] / X. Yang, J. Yuan, H. Yang, Y. Kong, H. Zhang, J. Zhao // Future Internet. – 2023. – Vol. 15, No. 4. – P. 127. – Mode of access: https://www.mdpi.com/1999-5903/15/4/127 (date of access: 13.03.2026).
2. Javadpour, A. A Comprehensive Survey on Cyber Deception Techniques to Improve Honeypot Performance [Text] / A. Javadpour, F. Ja'fari, T. Taleb, M. Shojafar, C. Benzaïd // Computers & Security. – 2024. – Vol. 140. – P. 103792. – Mode of access: https://oulurepo.oulu.fi/bitstream/handle/10024/48484/nbnfioulu-202403262445.pdf (date of access: 14.03.2026).
3. Ilg, N. A Survey of Contemporary Open-Source Honeypots, Frameworks, and Tools [Text] / N. Ilg, P. Duplys, D. Sisejkovic, M. Menth // Journal of Network and Computer Applications. – 2023. – Vol. 220. – P. 103737. – Mode of access: https://www.sciencedirect.com/science/article/abs/pii/S108480452300156X (date of access: 14.03.2026).
4. Priya, V. S. D. Containerized Cloud-Based Honeypot Deception for Tracking Attackers [Text] / V. S. D. Priya, S. S. Chakkaravarthy // Scientific Reports. – 2023. – Vol. 13. – P. 1437. – Mode of access: https://www.nature.com/articles/s41598-023-28613-0 (date of access: 14.03.2026).
5. Outpost24. Cyber Threat Landscape Study 2023: Honeypot Findings From Over 42 Million Attacks [Electronic resource]. – 2023. – Mode of access: https://outpost24.com/blog/honeypot-findings-from-over-42-million-attacks/ (date of access: 14.03.2026).

6. Sokol, P. Honeypots and Honeynets: Issues of Privacy [Text] / P. Sokol, J. Míšek, M. Husák // EURASIP Journal on Information Security. – 2017. – Vol. 2017, No. 4. – Mode of access: https://jis-eurasipjournals.springeropen.com/articles/10.1186/s13635-017-0057-4 (date of access: 12.03.2026).

Немировська Дар'я Олександрівна – студентка групи 1БКС-22б, Факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, Україна, e-mail: nemyrovskadaria@gmail.com

Науковий керівник: ***Магас Людмила Миколаївна –*** *старший викладач кафедри іноземних мов, Вінницький національний технічний університет, e-mail: magas@vntu.edu.ua.*

Nemyrovska Daria Oleksandrivna - student of group 1BKS-22b, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, Ukraine, e-mail: nemyrovskadaria@gmail.com

Supervisor: ***Liudmyla Magas*** *– senior teacher of English, the Foreign Languages Department, Vinnytsia National Technical University, Vinnytsia, e-mail: magas@vntu.edu.ua.*