Honeypots: Concepts, Types, and Challenges

By Zeenat Nisa

***Abstract*—Cybersecurity remains a paramount concern in our rapidly evolving technological era. This paper supplies a comprehensive study of honeypots, a crucial tool in modern cybersecurity. This exploration examines the purpose, concepts, diverse types, advantages, disadvantages, and challenges associated with honeypots. Consequently, this paper offers a clear understanding of how honeypots function as a decoy system strategically placed within networks to prevent, detect, and gather information about malicious actors and activities.**

***Index Terms*—honeypots, honey nets, research honeypots, production honeypots, interaction levels.**

I. Introduction

In this era of rapid technological advancement, cybersecurity is imperative for individuals and organizations. As a result, comprehensive security measures and rigorous threat intelligence planning are essential, to reduce the risk of security breaches [21], [22]. This report will explore the fundamental concepts of honeypots, an integral tool in modern cybersecurity. Honeypots are strategically placed decoy systems, designed to attract and detect malicious activities before attackers can compromise critical systems. they help to enhance system security by analysing and mitigating threats. By doing so, honeypots supply valuable insight into the tactics and techniques used by malicious actors.

The following sections aim to delve into the primary concepts of honeypots and to discuss their types, and challenges associated with their implementation. The paper is structured as follows: Section 1 is the Introduction, Section 2 will explore the Concepts of Honeypots, Section 3 will cover the Types of Honeypots, Section 4 will cover the Advantages, Section 5 will discuss the disadvantages, Section 7 will explain the Challenges related to Honeypots and finally, Section 8 will conclude.

II. Concepts of Honeypots

This section discusses the core concepts of honeypots a dynamic technology with various roles in cybersecurity, including prevention, detection, and information gathering [20]. A honeypot is any system set up as a 'fake' system to detect unauthorised activity [3]. They can take various forms, including network routers, operating systems, services running on ports, devices, or entire systems. It is crucial to note that honeypots are not standalone solutions; rather, they are more effective when used in conjunction with other defence techniques such as Firewalls, Intrusion Detection Systems (IDS) or Encryption [1].

A. Purpose

The primary purpose of a honeypot is to function as an early warning system, detecting malware and hackers. Unlike many conventional security technologies, honeypots rely on interaction, intentionally designed to be deceptive and not attract legitimate connection attempts, [17] hence, a honeypot should not be used internally once it has been launched. After filtering out legitimate traffic, any remaining attempts are considered malicious. This quality acts as a reliable signal for any malicious behaviour for security professionals.

'Fig. 1" depicts an attacker attempting to access what they believe to be the organisation's genuine system. However, it is a decoy system strategically placed to deceive the attacker, allowing organisations to comprehend their techniques, and take proactive measures before the attacker gains access, as the attacker will be slowed down by honeypots. [14].

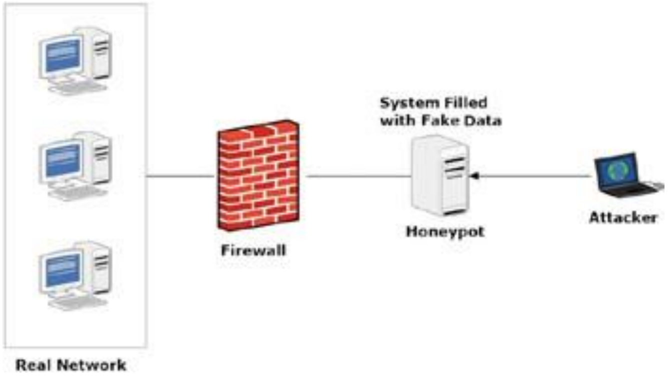

Fig. 1. Honeypot Security [14]

Honeypots offer effective intrusion detection, particularly when other defence approaches have been bypassed [8]. As hackers navigate through the system or network, they inevitably encounter honeypots. Consequently, the honeypot will detect the hacker, offering valuable insights into their techniques and unveiling potential threats.

B. Advance Honeypot Concepts

Moreover, advanced honeypot concepts have evolved to overcome the developing tactics of malicious hackers. These all share a common purpose, to detect malicious actors and gain insight into their behaviour [16]. A honeypot is meant to entice attackers to perform malicious activities and henceforth reveal information about their tactics, techniques, and procedures. Hence, honeypots are a formidable tool for preventing and mitigating different attacks [18].

Moving beyond honeypots, honey nets have emerged. A honey net is a collection of honeypots. Within this network, a

honey wall can act as a perimeter border between honey nets and the productive system. The honey wall evaluates incoming traffic, deciding whether traffic is deemed to be malicious, redirecting it to the honey net, or allowing it to continue to the productive system [15]. What's more, honey tokens can add another layer of security. Honey tokens are data elements, such as files, designed to appear valid and entice hackers. They produce an alert when modified or accessed, helping detect intrusion within systems [15].

Furthermore, honey farms simplify large-scale deployments of honeypots, offering a centralised approach to managing multiple honeypots. In a honey farm, traffic directing may be employed to direct potentially malicious traffic to third-party honeypots [21].

Data control, data capture, data collection, and data analysis are the four main components of a honey net [11].

Data control is the ability to control and restrain any malicious behaviour that occurs [11]. Data Capture is the process by which the honeypot keeps track of and records activities each time a hacker interacts with the system [23]. Data Collection is the process of keeping track of logs obtained from the attacker's interactions with the honey net. Data analysis involves carefully examining every piece of information that is gathered during the honey net's interaction with the attacker [11].

C. Best Practices for Effectively Deploying Honeypots

When implementing a honeypot, certain factors need to be considered, for efficient deployment and minimal risk [1]. These primary factors include:

- Type of Data Available: The data that will be used in the system will need to be considered, to ensure realism, warranting the legitimacy of the honeypot, and guarantee minimal risk, if the data is exploited.
- Effective Immediate Response: Measures should also be in place if the honeypot does catch an attacker. What will the next steps be?
- Preventing Uplink Liability: The honeypot should be closely monitored to prevent attackers from exploiting the honeypot to launch attacks against other systems.
- Build or Purchase Decision: This involves the decision of whether a honeypot is necessary, considering whether to build or purchase a honeypot and considering maintenance and expertise requirements for monitoring and examining honeypot data.
- Optimal Honeypot Location: Where is the most effective place for your honeypot? The honeypot should be placed in the organisation's real network, separate from other defence mechanisms, to protect other machines from the attackers [4].
- Utilising Mirrored Defence Systems: Mirror the defence strategies in the honeypot that are employed in regular systems within the organisation. This will help understand how attackers will infiltrate defences, helping to create effective mitigation strategies.

III. Types of Honeypots

Honeypots can be classified based on their purpose, interaction levels and deployment strategies.

A. Purpose-based Classification

In terms of purpose, honeypots can be classified into two main categories: production honeypots and research honeypots [5]. It is important to note that the classification between production and research honeypots can be fluid, and some honeypots may serve both purposes.

A research honeypot is often utilised, by researchers, to gain information about the attacker's intentions, and their tactics, techniques, and procedures [24]. Researchers can use this information to discover the latest attack trends, tools and strategies used. These honeypots are typically used by those more interested in learning about threats rather than those wanting to catch a hacker, such as universities. Research honeypots are extremely valuable to study cyber threats as they capture a large amount of data. The attackers can be analysed as they attack, step by step as they work through the network. However, research honeypots are difficult to deploy, and they are very time-consuming [1]. A research honeypot does not aim to benefit an organisation, with its main purpose being to obtain information [20].

There are many real-world examples of honeypot deployments. One instance is Project Honey Pot, initiated in 2004 to combat the rise of spammers and spambots exploiting website vulnerabilities to collect email addresses [6]. Through strategically placed honeypots across various websites, the project managed to collect a substantial amount of data on IP addresses associated with spam-related activities. The collected data aided in countering email harvesting attempts by understanding the techniques employed by spammers, offering efforts to mitigate spam and enhance security. With widespread adoption, Project Honey Pot also provides valuable data into spam-related activities [7].

A production honeypot is a honeypot which is deployed within the production network of a system. The production network refers to the operational network environment where significant business activities and operations take place. Production honeypots add to the security of an organisation. They aim to identify and detect malicious threats targeting the system, which could potentially impact the organisation. These insights can be used to mitigate these threats by building better defences against future threats, leaving organisations better prepared. They lure hackers to interact with them, allowing organisations to observe attack processes, identify vulnerabilities, and gain insights into the attack techniques [18].

Production honeypots are easier to build and deploy compared to research honeypots, as they offer less functionality and do not need to provide a high amount of information about the attacker [15]. Their main purpose is to detect and alert the threat of a hacker attempting to exploit a false vulnerability.

In a real-world example, in 2001, Incidents.org effectively employed a honeypot to capture and analyse the Leaves worm. This incident illustrates the effectiveness of honeypots in capturing and dissecting security threats but also plays a crucial role in heightening awareness within the security community [4].

B. Interaction Levels

Another way to classify honeypots can be based on their level of interaction, the need for the honeypot will reflect the level of interaction used. The interaction level reflects how well the honeypot replicates the real system. The levels of interactions are categorised as low, medium, and high. The choice of interaction level depends on the honeypot's goals, with lower levels being simpler to maintain, and higher levels proving more realistic [20].

A low-interaction honeypot imitates services that have restricted functionality and pose minimal risk as they cannot be fully taken over, for example emulating an FTP service and eavesdropping on port 21 [10]. As a result, the data generated is little, they are easier to deploy and, the risk associated with the honeypot deployment is shallow. They are mainly used for analysing spammers or against worms [20]. An example of a low-interaction honeypot is HoneyC. HoneyC is a lowinteraction client-based honeypot designed to mimic the key features of target clients. This allows it to detect and analyse client-side attacks, providing insights into the techniques used by hackers. [9]

Medium-interaction honeypots stimulate more complex services and generate a higher risk and more data, than lowinteraction honeypots, striving to provide a moderately realistic experience [25]. An example is 'Nepenthes.' This daemon detects automated attacks, extracts information from the attack, and subsequently downloads the identified malware, allowing professionals to study and analyse the malware.

High-interaction honeypots will imitate a real system so well that hackers find it difficult to distinguish it from a genuine asset, such as an authenticated and frequently updated website. The information provided by the honeypot is incredibly good and detailed. Due to their complexity, they are more time-consuming to design and have the highest level of risk. A honeynet is an example of a high-interaction honeypot due to its full emulation of systems [5].

C. Deployment Strategies

Deployment methods include using a real, unused system or utilising specialised software that emulates a system, at different levels of the Open Systems Interconnection model. For example, there are virtual honeypots and Physical honeypots. A physical honeypot is a tangible machine, often with high interaction, whilst a virtual honeypot is a software process, often with low interaction. Physical honeypots can be expensive to manage, and virtual honeypots are more costeffective. Virtual honeypots also offer the benefit of better separation and allow multiple honeypots to be running on a single machine [26]. Honeyd is an example of a virtual honeypot.

Honeypots can also be distinguished based on the different services they are mimicking, such honeypots as SSH honeypots, SMTP honeypots, FTP honeypots. [21]

IV. Advantages of Honeypots

In this section, we explore the numerous advantages associated with the implementation of honeypots. Honeypots offer benefits that enhance threat detection, intelligence gathering and a good overall security stance. The following are the advantages of honeypots, highlighting their importance in cybersecurity:

- Small Data Sets: Honeypots focus only on incoming traffic directly interacting with the honeypot, generating minimal yet highly valuable data. This focused approach avoids the issues of overwhelming amounts of data or dealing with a high number of alerts [1] [21].
- Enhanced Threat Intelligence and Security: Many honeypots can trace sources and destinations, serving as a strong tool to collect valuable information about the attacker, their employed tools and techniques. As a result, organisations can strengthen their defences against known attacks through analysing the honeypot data [1].

- Identification of Zero-Day Attacks: Honeypots excel at identifying zero-day attacks as the attacker may utilise a new technique whilst falling for the honeypot bait [4].
- Minimal Resource Requirements: As honeypots capture only malicious activity, they require minimal resources. Even retired, used systems can be employed as honeypots [11].
- Cost-Effective: Due to low resource requirements, honeypots tend to be cost-effective [21].
- Simplicity: Unlike more complex security solutions, honeypots do not require to development of complex algorithms or the maintenance of signatures. This makes them easy to deploy and manage [1].
- Discovery of New Tools and Tactics: Honeypots log any tools or tactics being utilised by the attacker. As a result, honeypots are exposed to a wide range of methods. Plus, attackers may unknowingly use new or previously unseen methods, providing valuable insights [1].
- Small Number of False Positives: Unlike an Intrusion Detection System (IDS), honeypots experience low traffic, and any detected traffic is likely to be malicious. Raising awareness of the honeypot within the organisation will generate fewer false positives as no one will intentionally interact with a honeypot [4].

V. Disadvantages

Honeypots while invaluable in enhancing cybersecurity strategies come with inherent challenges and risks that require consideration. This section explores the disadvantages associated with honeypot deployments.

- Limited Visibility: Honeypots only detect malicious activity when the attacker interacts with them. Therefore, potential malicious activity in other parts of the system will not be detected by the honeypot unless the attacker directly interacts with the honeypot [11].
- Discovery and Fingerprinting: The risk of the attacker discovering the honeypot exists. This is often due to mistakes such as a misspelt word can expose the honeypot. This can hinder the usefulness of the honeypot. If detected, the value of the honeypot diminishes [27]. This can lead to the attacker potentially feeding fake information to the honeypot which can mess up research honeypot data and insights.
- Risk of Takeover: If discovered, the attacker can attempt to take over the honeypot and if successful they may use it to deploy subsequent attacks on their systems [4]. The more complex the honeypot, the greater the fallout could be.
- Real-Time Prevention Challenge: Although effective for studying attacks after they occur and helping to implement recommendation strategies. Production honeypots are not handy for preventing attacks before they happen as they detect the attacker in the process of the attack
  [20].

VI. Legal, Ethical and Professional Challenges

The usage of honeypots is not without its legal, ethical and professional issues, these demand careful attention.

A. Legal Issues

The legal implications of deploying honeypots mainly include claims of entrapment, privacy rights and liability.

Entrapment refers to the attacker claiming that the honeypot coerced them to commit the crime and would not have done so without it [21]. However, Ronald L. Spitzner argues honeypots, when utilised for defensive purposes, do not actively coerce criminal behaviour [15].

Honeypots involve the collection of data and the stringent laws for this need to be followed by organisations. As a result, compliance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 is imperative [12]. Obtaining consent for data collection is crucial and honeypots may involve users unknowingly contributing data. Therefore, the purpose of the honeypot and data collection must be clear, and the data collected should be used solely for the specified purpose with the minimum amount of data collected as possible.

Honeypots, if compromised, may pose a liability risk, as mentioned previously. The honeypot could be manipulated, by attackers, to launch further attacks. This potential misuse could lead to accusations against the honeypot deployer, hence robust security measures are needed to prevent unauthorised takeovers.

B. Ethical Issues

The ethical risks involved in honeypot deployment include the risk of unauthorized access to the honeypot by attackers, which could lead to the compromise of sensitive information. Additionally, the deceptive nature of honeypots must not cause harm and only be implemented for legitimate purposes [21].

C. Professional Issues

The professional issues of honeypots include the need for proper training, adherence to cybersecurity guidelines and expertise to ensure proper utilisation and management.

Honeypots should be deployed only when the above aspects are considered [28] [13]. Honeypots when deployed for legitimate reasons in the interest of cybersecurity, hacker detection and user protection, align with the recommended standards.

VII. Conclusion

In conclusion, this paper broadly discussed honeypots, exploring their concepts, types, and associated challenges. By examining, both the advantages and disadvantages, including legal, ethical, and professional considerations, a comprehensive understanding of Honeypots was achieved. Honeypots stand as beneficial technologies, effective in detecting cyber threats and attackers. However, they prove more effective when used in conjunction with other cyber tools, improving our ability to understand attacker techniques and methods. Honeypots play a crucial role in adapting response and mitigation strategies. Ultimately, Honeypots have not only proved effective in threat detection but have also significantly contributed to the ongoing evolution of cybersecurity.

References

[1] I. Mokube and M. Adams, “Honeypots: concepts, approaches, and challenges,” Proceedings of the 45th annual southeast regional conference on - ACM-SE 45, pp. 321–326, Mar. 2007, doi: https://doi.org/10.1145/1233341.1233399.

[2] GOV.UK, “Cyber Security Breaches Survey 2022,” GOV.UK, Mar. 30, 2022. https://www.gov.uk/government/statistics/cyber-security-breachessurvey-2022/cyber-security-breaches-survey-2022

[3] R. A. Grimes, Hacking the Hacker. Indianapolis, Indiana: John Wiley and Sons, Inc., 2017. doi: https://doi.org/10.1002/9781119396260.

[4] Mohssen Mohammed and Habib-Ur Rehman, Honeypots and Routers Collecting Internet Attacks. Auerbach Publications, 2015.

[5] Diab, D. M., AsSadhan, B., Binsalleeh, H., Lambotharan, S., Kyriakopoulos, K. G., & Ghafir, I. (2019, August). Anomaly detection using dynamic time warping. In 2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC) (pp. 193-198). IEEE.

[6] Karthik Sadasivam, Banuprasad Samudrala, and T. Yang, “Design of network security projects using honeypots,” Journal of Computing Sciences in Colleges, vol. 20, no. 4, pp. 282–293, Apr. 2005, doi: https://doi.org/10.5555/1047846.1047890.

[7] B. B. Gupta and A. Gupta, “Assessment of Honeypots,” International Journal of Cloud Applications and Computing, vol. 8, no. 1, pp. 21–54, Jan. 2018, doi: https://doi.org/10.4018/ijcac.2018010102.

[8] Lefoane, M., Ghafir, I., Kabir, S. and Awan, I.U., 2021, December. Machine learning for botnet detection: An optimized feature selection approach. In The 5th International Conference on Future Networks & Distributed Systems (pp. 195-200).

[9] M. Prince et al., “Understanding How Spammers Steal Your E-Mail Address: An Analysis of the First Six Months of Data from Project Honey Pot,” Jul. 2005. Accessed: Dec. 14, 2023. [Online]. Available: https://www.ceas.cc/papers-2005/163.pdf

[10] H. Al-Mohannadi, I. U. Awan, J. Al Hamar, A. J. Cullen, J. P. Disso, and L. Armitage, “Cyber Threat Intelligence from Honeypot Data using Elasticsearch,” bradscholars.brad.ac.uk, May 18, 2018. https://bradscholars.brad.ac.uk/handle/10454/16385.

[11] Eltanani, S. and Ghafir, I., 2020, November. Coverage Optimisation for Aerial Wireless Networks. In 2020 14th International Conference on Innovations in Information Technology (IIT) (pp. 233-238). IEEE.

[12] I. Welch, P. Komisarczuk, R. Holloway, and C. Seifert, “HoneyC -The Low-Interaction Client Honeypot HoneyC -The Low-Interaction Client Honeypot HoneyC -The Low-Interaction Client Honeypot,” 2007.

[13] H. Artail, H. Safa, M. Sraj, I. Kuwatly, and Z. Al-Masri, “A hybrid honeypot framework for improving intrusion detection systems in protecting organizational networks,” Computers Security, vol. 25, no. 4, pp. 274–288, Jun. 2006, doi: https://doi.org/10.1016/j.cose.2006.02.009.

[14] Zhang, Y., Yang, Q., Lambotharan, S., Kyriakopoulos, K., Ghafir, I. and AsSadhan, B., 2019, October. Anomaly-based network intrusion detection using SVM. In 2019 11th International conference on wireless communications and signal processing (WCSP) (pp. 1-6). IEEE.

[15] J. Labar, M. Chowdhury, M. Jochen, and K. Kambhampaty, “Honeypots: Security by Deceiving Threats,” Apr. 2018. Accessed: May 30, 2023. [Online]. Available: https://www.micsymposium.org/mics2019/wpcontent/uploads/2019/05/HoneyPots.pdf

[16] P. Sokol, J. M´ısek, and M. Husˇ ak, “Honeypots and honeynets: issues of´ privacy,” EURASIP Journal on Information Security, vol. 2017, no. 1, Feb. 2017, doi: https://doi.org/10.1186/s13635-017-0057-4.

[17] R. Campbell, “The Legal and Ethical Issues of Deploying Honeypots Honours Project (INF412-H),” Mar. 2014.

[18] Eltanani, S. and Ghafir, I., 2021, May. Aerial Wireless Networks: Proposed Solution for Coverage Optimisation. In IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 1-6). IEEE.

[19] N. A. Hassan, Ransomware revealed : a beginner’s guide to protecting and recovering from ransomware attacks. New York: Apress, 2019.

[20] L. Spitzner, Honeypots : tracking hackers. Boston: Addison-Wesley, 2003.

[21] P. Lackner, “How to Mock a Bear: Honeypot, Honeynet, Honeywall and Honeytoken: A Survey,” Proceedings of the 23rd International Conference on Enterprise Information Systems, 2021, doi: https://doi.org/10.5220/0010400001810188.

[22] Lefoane, M., Ghafir, I., Kabir, S. and Awan, I.U., 2022. Unsupervised learning for feature selection: A proposed solution for botnet detection in 5g networks. IEEE Transactions on Industrial Informatics, 19(1), pp.921-929.

[23] A. B. R. Petrunic, “Honeytokens as active defense — IEEE Conference´ Publication — IEEE Xplore,” ieeexplore.ieee.org, May 2015.

[24] N. Titarmare, N. Hargule, and A. Gupta, “An Overview of Honeypot Systems,” International Journal of Computer Sciences and Engineering, vol. 7, no. 2, pp. 394–397, Feb. 2019, doi: https://doi.org/10.26438/ijcse/v7i2.394397.

[25] M. Kofler et al., Hacking and Security. SAP Press, 2023.

[26] Aparicio-Navarro, F.J., Kyriakopoulos, K.G., Ghafir, I., Lambotharan, S. and Chambers, J.A., 2018, October. Multi-stage attack detection using contextual information. In MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM) (pp. 1-9). IEEE.

[27] A. A. N. Naeem, “Honeypots: Concepts, Approaches and Challenges,” hal.science, Aug. 23, 2021. https://hal.science/hal-03324407

[28] L. Zobal, D. Kola´ˇr, and R. Fujdiak, “Current State of Honeypots and Deception Strategies in Cybersecurity,” IEEE Xplore, Oct. 01, 2019.