PREVENTIVE INTERNAL ATTACKS USING HONEYPOTS WITH TRAPS IN CYBERSECURITY

By Augastine Ndeti

ACKNOWLEDGEMENT

I wish to extend my heartfelt appreciation to the people and organisations whose unwavering support and guidance have been invaluable to me throughout my dissertation research. Without their assistance, this project would not have been possible.

My sincere gratitude goes to my advisor, Joseph, whose mentorship, expertise, and encouragement were instrumental in successfully completing this dissertation. In particular, he provided me with valuable guidance and support throughout my dissertation research. He provided me with constructive feedback and advice on my research proposal and project plan, which helped me to refine my ideas and focus my research. He also assisted me in navigating the research process, from developing a detailed timeline to establishing a structured research methodology. He regularly gave me in-depth feedback on my progress, and provided insightful guidance on the challenges I faced. He made himself available to answer any questions I had and motivated me to stay on track. His expertise and unwavering support were instrumental in helping me complete the project successfully.

I would also like to express my appreciation to the members of my dissertation committee, Johnny, Garlsen Moon, and Tommy, for their constructive feedback and insightful comments on my work.

Furthermore, I am indebted to the faculty of the Computer Science and Engineering Department of the University, my peers, and the research staff at the Cybersecurity Research Center; for providing me with financial, technical, and logistical support for this project, that was critical to the success of my research.

Lastly, I am deeply grateful to my family and friends for their unwavering support and encouragement throughout this challenging journey. Their love and belief in me kept me motivated and inspired to reach the finish line.

Abstract

Honeypots and cybersecurity are two concepts that are closely related. Honeypots are a type of cybersecurity technology that is designed to attract and trap cyber attackers. They are essentially decoy systems that are set up to mimic real systems or networks, with the goal of luring in attackers and studying their behaviour. Honeypots are used by cybersecurity professionals to gather valuable information about attackers, such as their tactics, techniques, and procedures (TTPs). The primary purpose of honeypots is to gather information about attackers that can be used to improve an organisation's overall cybersecurity posture. By understanding how attackers operate, organisations can better prepare for and defend against cyber-attacks. Honeypots can also be used to distract attackers from real systems and networks, reducing the likelihood of a successful attack. Cybersecurity is a term used in the IT industry to describe a range of measures taken to prevent data breaches and other forms of cybercrime. The implementation of various technologies, methods, and procedures is required to ensure the security, availability, and privacy of digital assets. In cybersecurity, a preventative method of attack involves the use of honeypots equipped with traps as a form of decoy system. The purpose of this research proposal is to examine the feasibility of using honeypots equipped with traps to protect businesses from cyberattacks launched from within. A software program that can create honeypots with traps and give insights into the behaviour of attackers is the predicted practical outcome of this research. The success of the honeypots in thwarting internal cyberattacks will be analysed and reported on as well. The research will yield a contribution to the field of cybersecurity and will necessitate a deep comprehension of cybersecurity concepts and principles, familiarity with network architecture and protocols, skill with programming and scripting languages, and expertise with virtualisation and containerisation technologies.

Table of Contents

Chapter 1: Introduction

The introductory chapter of this research provides a comprehensive overview of the entire study. It covers all the major concepts that are relevant to the research. This chapter includes a detailed introduction to the research topic, the research background, and an overview of the company on which the research is based. Additionally, the chapter outlines the aim of the research, its objectives, and the specific research questions that have been developed for this study. The content of this chapter is essential and serves as the foundation for the research study. It sets the tone and direction for the entire research project. The introductory chapter provides an in-depth explanation of the research topic and background, which is crucial for readers to understand the context of the study. Moreover, this chapter explains the significance of the research questions and how they relate to the research objectives. The research questions are designed to guide the research and provide a framework for the study's findings. Therefore, it is essential to have a clear understanding of the research questions before beginning the study. Finally, the introductory chapter outlines the scope of the research and provides a brief overview of the other chapters that are included in the dissertation. This section helps the reader to understand what to expect from the study and how the research is organised.

1.1 Research Introduction

According to Mayorga et al. (2019), one of the primary challenges in preventing internal attacks is the lack of visibility into malicious behaviour, inadequate proactive measures to prevent malicious insiders from accessing sensitive systems, and limited resources for detecting and responding to incidents. Malicious insiders can be difficult to detect as they may use legitimate credentials to bypass security measures and gain access to critical systems. The complexity of IT systems, the increasing use of cloud computing, and mobile devices have only exacerbated this challenge. Moustafa and Slay (2016) state that honeypots have evolved significantly in the cybersecurity industry. While they were initially used to attract and detect malicious actors, they have become more sophisticated and are now utilised for both detection and prevention of malicious activities. Low-interaction honeypots are used to detect malicious actors by monitoring their behaviour and analysing traffic patterns, while high-interaction honeypots are used to lure and trap malicious actors. Honeyclients are also used to detect malware propagation, and honeypots can detect malicious insiders in critical infrastructures. The use of honeypots with traps in cybersecurity research is particularly relevant today as it offers a comprehensive approach to detect and prevent malicious insider activity (Sarfaraz et al., 2022). Honeypots with traps can identify malicious activity, actors, and prevent the spread of malware. Using honeypots with traps can also provide improved visibility into malicious activities and a proactive approach to preventing malicious attacks. The benefits of using honeypots with traps are numerous. They can be used to detect and analyse malicious activities, identify malicious actors and their tactics, and prevent the spread of malware. They can also detect malicious insiders in critical infrastructures, and provide improved visibility into malicious activities (Pellegrino, Giacinto and Sansone, 2010). By utilising honeypots with traps, organisations can gain improved visibility into malicious activities and take a proactive approach to preventing malicious attacks.

1.2 Research Background

The field of security is in a constant state of flux, with new developments and recommendations surfacing daily to combat the growing number of cybersecurity threats. A prominent trend in the security industry is the integration of artificial intelligence and machine learning techniques. These approaches allow for the analysis of substantial amounts of data in real-time, enabling prompt detection of anomalies and swift responses to security breaches. Additionally, the employment of cloud-based security solutions is becoming increasingly popular, as it affords more flexibility and scalability than traditional on-premises solutions. Another fundamental best practice in security is the adoption of a zero-trust security model. The zero-trust model assumes that all devices and users within a network are potentially malicious and untrustworthy, necessitating continuous authentication and authorisation checks. This methodology can significantly decrease the likelihood of unauthorised access to critical systems and data, making it a crucial element of any modern security strategy (AlZoubi and Alrashdan, 2022). In addition, there is an increasing emphasis on enhancing security awareness and training among personnel. Human error remains one of the most significant cybersecurity hazards. Therefore, educating staff on how to identify and react to security threats is crucial. Educating employees to recognise phishing emails, report suspicious activities, and adhere to security best practices can help to reduce the likelihood of cyber-attacks.

The use of honeypots has proven to be an effective technique for detecting and analysing cyber threats. Today, various cyber-attacks can be prevented by utilising honeypots equipped with traps. However, it is critical to ensure that honeypots are kept up to date and do not become a security risk themselves. One of these attacks is the infamous malware attack, which can be addressed by using honeypots that collect samples of malware and examine their behavioural and characteristic traits. With this information, security personnel can develop new strategies to prevent the spread of malware by creating new signatures. In addition, honeypots with traps can detect and block traffic from recognised malicious IP addresses, which makes it an effective method to prevent distributed denial-of-service (DDoS) attacks. Insider attacks are another type of cyber-attack that can be thwarted using honeypots (Casola, D'Antonio and Romano, 2012). By constructing decoy systems that are solely accessible to authorised personnel, honeypots can identify unauthorised access and trigger an alert. This event will allow the security team to investigate the incident and take preventive measures. Lastly, phishing attacks can be prevented by honeypots equipped with traps that redirect attackers to decoy systems that record their login credentials. By redirecting attackers to such systems, honeypots reduce the risk of a successful phishing attack. As per Li and Ren (2022), deploying honeypots equipped with traps is a viable approach to thwarting attacks on critical infrastructure. These systems are capable of identifying and stopping attacks on industrial control systems (ICS) by emulating ICS decoy systems. Should an attacker attempt to infiltrate the ICS, the honeypot will raise an alarm, enabling the security team to analyse the situation. Additionally, honeypots with traps can be used to detect and thwart attacks on cloud computing environments by mimicking cloud environments through decoy systems.

Honeypots have been employed across various settings like enterprise networks, critical infrastructures, cloud computing environments, and home networks. Within enterprise networks, honeypots aid in the detection and analysis of attacks that may bypass traditional security measures such as firewalls and intrusion detection systems. They can also be used to draw attackers away from vital assets and provide valuable insight into their techniques and motives. Furthermore, honeypots play a crucial role in training security personnel and evaluating the efficacy of security measures. In critical infrastructures like power plants, water treatment facilities, and transportation systems, honeypots serve the purpose of identifying insider threats and external attacks. These honeypots can be situated at different points of the infrastructure to monitor and scrutinise traffic, thus helping in recognising anomalous activities and potential attacks. Additionally, honeypots aid in gathering intelligence on the attacker's abilities and motives, which can assist in developing countermeasures (Gharib, Slay, and Moustafa, 2020). Cybersecurity threats are not limited to traditional IT environments, as cloud computing platforms have also become targets of malicious actors. Fortunately, honeypots can aid in identifying and investigating such attacks within cloud computing setups. Honeypots can simulate weak points and entice hackers away from genuine services. Not only can honeypots recognise assaults against virtual machines and containers, but they can also help shield cloud-based systems and data. Honeypots have value outside of commercial setups as well, such as in household IoT networks. IoT devices are vulnerable to hacks, and honeypots can provide early detection of these attempts and stop them from spreading to other devices in the network. Additionally, honeypots can help build a profile of attackers and their objectives, which can support the creation of defense measures.

Cybersecurity professionals rely on honeypots to safeguard their systems against cyber-attacks. Nevertheless, the implementation of honeypots can be a challenging task that presents several limitations. Firstly, the cost of installing and maintaining honeypots can be exorbitant. It may entail a significant investment in hardware, software, and trained personnel, which could make it difficult for small organisations to effectively implement them (Kolawole, 2019). Secondly, honeypots may not always be effective in detecting attacks, especially when attackers employ sophisticated techniques to evade them. Additionally, attackers may avoid honeypots that are well-known, rendering them useless in detecting new and emerging threats. Hence, organisations need to keep their honeypots updated and deploy them in different locations to increase their chances of detecting attacks (Mayorga et al., 2019). The risk of false positives and false negatives is another limitation. False positives happen when a honeypot identifies legitimate traffic as an attack, while false negatives occur when a honeypot fails to detect an attack. False positives could lead to wastage of resources, whereas false negatives could result in severe damage to the organisation. As a result, organisations must configure honeypots to minimise the possibility of false positives and false negatives (Rajaboyevich et al., 2022). Lastly, honeypots may serve as an attack vector against an organisation. If a perpetrator gains entry to a honeypot, they can exploit it to launch attacks on other systems within the organisation or utilise the data obtained to launch attacks on other organisations. Therefore, organisations must guarantee that they establish robust security measures to safeguard

their honeypots from being breached. Generally, organisations should be cognizant of the potential constraints and obstacles associated with installing honeypots. They should devote adequate resources to ensure efficient implementation and maintenance of honeypots, set up multiple honeypots in different locations, configure honeypots to minimise the likelihood of false positives and false negatives, and establish robust security measures to safeguard their honeypots from being compromised.

Honeypots equipped with traps serve as a formidable defense mechanism against internal attacks. A honeypot is essentially a network-based system that replicates the functioning of an authentic system to lure attackers into interacting with it. With the added feature of traps, honeypots can be configured to identify and capture attackers who try to exploit vulnerabilities within the system. The captured information can comprise the attacker's IP address, operating system, and browser, among others. This data can then be used to identify the attacker and prevent future attacks. Honeypots with traps can go a long way in preventing internal attacks by enabling detection and tracking of malicious activities within the network. By deploying honeypots on internal systems, security teams can monitor and scrutinise the actions of internal users, including employees, contractors, and vendors. This approach can help in identifying and thwarting malevolent activities, such as data theft or unauthorised access to sensitive information. Furthermore, honeypots with traps can help detect and prevent lateral movement within the network by monitoring and documenting activities on the honeypot system. Additionally, honeypots equipped with traps offer an effective means for organisations to counteract attacks by providing valuable data on the tactics, techniques, and procedures used by attackers. By scrutinising the information gathered from honeypots, security teams can gain insight into the nature of the attacks employed, the vulnerabilities exploited, and the attack methods. This information can be used to update security policies, procedures, and defences in order to avert future attacks. In addition, honeypots can be used to assess the effectiveness of security controls and defences by exposing them to simulated attacks (Liu et al., 2022). Moreover, honeypots with traps can serve as an effective tool for educating and training employees on cybersecurity best practices. By simulating attacks with honeypots, employees can learn how to recognise and respond to actual threats. Honeypots can also be utilised to train incident response teams on the appropriate procedures for investigating and responding to cyberattacks. Overall, honeypots with traps can prove to be an indispensable part of an organisation's cybersecurity strategy, providing an extra layer of defense, detection, and deception.

1.3 Honeypots in Cybersecurity

Honeypots can be classified based on their degree of interaction with attackers, with three primary types available: low-interaction honeypots, medium-interaction honeypots, and high-interaction honeypots. The low-interaction honeypots are built to replicate the services of a specific operating system, such as HTTP or FTP. They are straightforward to set up and maintain but are not as effective in identifying sophisticated attacks because of their limited interaction capabilities (Nsiah-Konandu, Adu-Boahene, and Nikoi, 2022). On the other hand, medium-interaction honeypots are designed to replicate a more comprehensive range of services, and

they can interact with attackers at a deeper level than low-interaction honeypots. They require more resources and are moderately complicated to set up and maintain compared to low-interaction honeypots. Lastly, high-interaction honeypots offer attackers the most realistic environment for interacting with a simulated system or network. They require significant resources and expertise to set up and maintain but can provide comprehensive information about an attacker's behaviour and tactics (Camino et al., 2020).

The process of establishing a honeypot system involves various stages. First, it is essential to define the objectives and goals of the honeypot system. This necessitates recognising the types of attackers that the system aims to entice and the information it intends to gather. Subsequently, it is vital to choose the most appropriate type of honeypot that aligns with the system's objectives and goals. This entails assessing the extent of interaction the system needs with attackers and the resources available for deployment and upkeep (Camino et al., 2020). The third stage entails designing and configuring the honeypot system. This involves setting up the operating system, installing necessary software and configuring network connections. In the fourth stage, the honeypot system is deployed by positioning it in the network and configuring it to imitate a vulnerable system or service. Lastly, the honeypot system's data is monitored and analysed to identify any suspicious behaviour or patterns that may indicate an attack. This necessitates scrutinising the logs and identifying any suspicious activities.

Integrating honeypots into existing security infrastructures can be accomplished by deploying them on a separate network segment, such as a DMZ. This practice ensures that honeypots can be monitored independently of the production network, thereby allowing for the identification and analysis of any suspicious activity or attacks, without putting the production network at risk. By integrating honeypots with intrusion detection and prevention systems (IDPS), organisations can enhance their detection capabilities. For instance, honeypots can be useful in identifying zero-day attacks, which IDPS may not be able to detect due to the lack of a known signature. In addition, honeypots can also help identify attacks that may have bypassed existing security measures, such as firewalls, by creating a decoy target for attackers. Organisations can implement honeypots effectively by creating honeypots that accurately emulate their production systems, thus luring attackers to them. To minimise false positives, honeypots should be configured precisely to mimic the production systems. Furthermore, honeypots should have a high degree of interaction, encouraging attackers to spend more time interacting with them, thereby increasing the chances of capturing valuable information about the attacker's tactics and techniques. Regular monitoring and analysis of the data collected by honeypots can significantly reduce false negatives. It is also essential to keep the honeypots up to date with the latest software and security patches to prevent attackers from exploiting known vulnerabilities.

Relevance of the Research Topic:

Honeypots are a valuable tool in identifying and thwarting internal cyber-attacks. Spitzner (2003) found that honeypots are useful in detecting and preventing insider threats by attracting and monitoring the activities of privileged users who may be engaging in malicious behaviour. As reported Pellegrino et al. (2010), honeypots

have also been found to be effective in identifying new and unknown malware that may have evaded traditional cybersecurity measures, such as anti-virus software. However, the effectiveness of honeypots in preventing internal attacks hinges on their implementation and deployment. According to Moustafa and Slay (2016), for example, low-interaction honeypots may not be effective in identifying advanced persistent threats (APT), which necessitate a high level of interaction to detect. In comparison to conventional cybersecurity measures like firewalls and anti-virus software, honeypots are proactive rather than reactive. They attract attackers and enable the detection of attacks that may have bypassed existing security measures. Nonetheless, implementing and maintaining honeypots may be more resource-intensive than traditional cybersecurity measures. Additionally, the efficacy of honeypots may be limited if attackers are aware of their presence and take measures to avoid them. As a result, organisations should use honeypots in conjunction with other cybersecurity measures to achieve a comprehensive security strategy.

1.4 Research Aim and Research Objectives

The primary objective of this research project is to explore the efficacy of honeypots as a proactive strategy for identifying and mitigating internal cyber-attacks. To accomplish this aim, a set of research objectives has been established, which are as follows:

- To evaluate the effectiveness of honeypots in detecting and preventing different types of cyber-attacks, including insider threats, malware propagation, and unknown malicious attacks.
- To assess the challenges and opportunities associated with honeypot technology and their applications.
- To analyse the different types of honeypots and their deployment strategies in critical infrastructures and cloud computing environments.
- To identify the best practices for configuring and managing honeypots for optimal performance and threat intelligence.
- To propose a novel honeypot approach for network security and evaluate its effectiveness in detecting and preventing cyber-attacks.

The study's goals will be assessed and appraised by applying a range of metrics, including the detection rate, false positive rate, attack payload analysis, attack origin analysis, attack frequency, and threat intelligence analysis. Such metrics are crucial in gauging the efficiency and effectiveness of honeypots in detecting and thwarting cyber-attacks. Furthermore, they can provide valuable insights into the performance and deployment of honeypots across diverse scenarios.

The data collection techniques and tools that will be used to support the research objectives include:

- Honeypot deployment in different environments, such as critical infrastructures and cloud computing environments.
- Network traffic analysis using tools such as Wireshark and tcpdump to capture and analyse attack payloads and their origins.

- Log analysis of honeypot events and activities to identify attack patterns and behaviours.
- Threat intelligence analysis using open-source feeds and tools to gather and analyse information about new and emerging threats.

The research findings will inform future investigations by providing valuable insights into the efficacy and constraints of honeypots as a proactive technique for detecting and preventing cyber-attacks. The innovative honeypot approach proposed in this study can undergo further evaluation and refinement to enhance its performance and suitability for different contexts. Additionally, the research can be expanded to explore the integration of honeypots with other security mechanisms like intrusion detection and prevention systems to establish a holistic defense against cyber threats. Moreover, the research identifies best practices that can guide the deployment and management of honeypots in real-world situations to strengthen network security and threat intelligence. These findings hold significant implications for the field of cybersecurity, providing a foundation for future research and development.

1.5 Research Question

The following research questions have been formulated for this study:

- **How successful are honeypots with traps in avoiding internal cyber-attacks?**
- **What are the potential challenges associated with implementing honeypots with traps?**
- **How can honeypots with traps be integrated into an existing security infrastructure?**
- **What metrics should be used to evaluate the effectiveness of honeypots with traps?**
- **What is the expected practical element output from this research project?**

The objectives, as well as the research question developed above, will be supported by theory provided in later chapters of the study. This will be accomplished through a thorough examination of the information gathered in accordance with the research strategy that has been established for this study.

1.6 Purpose of Research Study

This research paper titled “Preventive Internal Attacks Using Honeypots with Traps in Cybersecurity” is a valuable addition to the cybersecurity domain. Insider attacks pose a significant risk to organisations, making it imperative to prevent them to safeguard confidential information and systems. Honeypots have proven to be an effective tool for detecting and analysing attacks. However, their potential for preventing insider attacks is yet to be fully explored. The study aims to examine the use of honeypots with traps to prevent internal attacks. The research findings can help organisations develop efficient preventive measures against insider attacks, thereby protecting them from substantial financial losses, damage to their reputation, and legal repercussions.

Through investigating the usage of honeypots with traps for deterring insider assaults, this research project will add to the body of existing knowledge. Past research has concentrated on the use of honeypots to gather malware samples and identify attacks. The suggested study advances the field of attack prevention by

investigating the use of honeypots. The study will look into how well honeypots with traps work to stop internal attacks and will determine the ideal setup for the best outcomes.

1.7 Research Scope

The goal Scope of this study is to better understand how using honeypots with traps might guard against internal cyber intrusions. Specifically, the research aims to evaluate the effectiveness of honeypots in detecting and preventing insider threats in various types of organisations. The study will focus on low-interaction honeypots that simulate vulnerabilities to attract attackers and traps that are designed to detect and disrupt attacks. The research project will also explore the challenges and limitations of using honeypots and traps in preventing internal attacks, and propose strategies to address these issues. The geographical region that will be covered by this research study is a global scope. Based on the references used for this dissertation, the research is likely to have a global perspective as it draws on studies from different regions including Europe, the United States, and Asia. The research project will study various types of organisations that are susceptible to insider threats, including critical infrastructures, cloud computing environments, and networks with unknown malicious attacks. The studies cited in the reference list suggest that the research will include both public and private sector organisations, such as government agencies, financial institutions, and healthcare providers. The research will involve a combination of quantitative and qualitative data. This may include data on the effectiveness of honeypots in detecting and preventing internal attacks, the frequency and types of attacks, and the costs associated with implementing and maintaining honeypots. The research may also involve qualitative data such as scientific publications with cybersecurity professionals and analysis of case studies to identify best practices and strategies for preventing internal attacks.

1.8 Research Outline

This is a quick breakdown of each of the research chapters:

Chapter 1: Introduction

This chapter serves as the introduction to the research study and provides a comprehensive overview of the important concepts that will be explained in further detail. It is essential to highlight these fundamental concepts as they form the basis of the entire research project. As a result, this introductory chapter is considered integral to the research and the most crucial chapter. In this chapter, the research aim, objectives, and research questions will be determined. These concepts will be supported by evidence collected in the subsequent chapters of the research study.

Chapter 2: Literature Review

As a means of protecting against cyberattacks from within, honeypots with traps will be thoroughly evaluated in this chapter. This evaluation will look particularly closely at honeypots as a safeguard against hacking from

within an organisation. It will explore the history of honeypots and their evolution into a security mechanism. It will also discuss the potential challenges and limitations associated with their implementation.

Chapter 3: Research Methodology

This chapter will outline the research methodology to be used in the project. It will discuss the research questions to be answered and the research design to be used. Additionally, it will describe the simulation environment to be set up to evaluate the software tool and the data collection and analysis techniques to be used.

Chapter 4: Software Tool

This chapter will provide a detailed description of the software tool to be developed as part of the project. It will include an overview of the software architecture and an explanation of the features and functionalities of the tool. It will also provide details on the technologies used to develop the tool and the programming languages used.

Chapter 5: Framework

This section outlines the framework for deploying honeypots with traps in an organisational environment. It includes instructions and recommended practices for configuring and establishing honeypots, as well as suggestions for integrating the honeypot system with the current security infrastructure. Moreover, the section covers the metrics used to assess the efficacy of the honeypot system.

Chapter 6: Simulation and Evaluation

This chapter will discuss the simulation environment to be set up to evaluate the software tool. It will explain the different attack scenarios to be simulated and the metrics to be used to evaluate the effectiveness of the honeypot system. Additionally, it will provide details on the data collection and analysis techniques to be used.

Chapter 7: Discussion and Conclusion

This chapter will discuss the implications of the research project and provide a conclusion. It will summarise the main findings of the research study and discuss the potential applications of the software tool and the framework developed. The chapter will also provide recommendations for future research.

1.9 Research Limitations

- Potential limitations of this research project include the complexity of the honeypot system, the possibility of false positives and false negatives, and the difficulty of correlating attacks across different honeypots. There is also the possibility that attackers may be able to bypass the honeypots and access the production systems.

- Challenges may arise due to the scope and timeframe of the research, such as the need to develop a comprehensive software tool within a limited timeframe, the complexity of the simulation environment, and the need to analyse a large amount of data.
- Ethical considerations may bring challenges during the research, such as the need to ensure that the honeypot systems are set up securely and that the data collected is handled responsibly. Additionally, there is the potential for privacy issues to arise if the honeypots are configured to capture sensitive information.

Chapter 2: Literature Review

2.1 History and Evolution of Honeypots in Cybersecurity Research

Honeypots have become a popular technology in cybersecurity research, and they have been around for decades. The first-ever honeypot was developed in 1989 by Clifford Stoll, a computer security researcher at Lawrence Berkeley National Laboratory. Stoll designed the honeypot to catch a hacker who had infiltrated the laboratory's computer network. After successfully capturing the hacker, the use of honeypots in cybersecurity was born (Zymberi, 2021). Since the development of the first honeypot, the concept has evolved significantly. Modern honeypots have several capabilities that earlier versions lacked. Today, honeypots are used to identify and analyse cyber-attacks and understand attackers' behaviour and motivations (Amal and Venkadesh, 2022).

Over the years, honeypots have been utilised for various purposes in cybersecurity research. Honeypots have been used to detect and analyse malware, identify attack patterns and trends, and study attackers' behaviour. They have also been used to deceive attackers into revealing their tactics and techniques and distract them from actual targets (Maesschalck et al., 2021). One of the significant capabilities of honeypots is that they are non-intrusive, meaning they do not interfere with the regular operations of a system or network. Traditional security measures can sometimes miss attacks, but honeypots can detect them, providing a safe environment for attackers to interact with, allowing researchers to study their behaviour and develop effective countermeasures (Mohan et al., 2022). Various types of honeypots have been developed over the years, each with its unique abilities and limitations. For instance, Shi et al. (2021) describe array honeypots, which are a collection of honeypots working together to detect and respond to attacks. The authors suggest that using evolutionary game theory can optimise array honeypots to improve their effectiveness in detecting attacks. The evolution of honeypots will undoubtedly continue, and the technology field can expect to see more advanced versions in the future.

Experts in the field of cybersecurity have highlighted various outcomes of using honeypots, according to their respective research. Mashima et al. (2020) noted that honeypots are primarily used for the collection of threat intelligence. By analysing data collected from honeypots, organisations can gain valuable insights into the behaviour of attackers, their tactics, techniques, and procedures (TTPs), and the vulnerabilities they exploit. Hassan et al. (2021) added that honeypots can be used for content moderation, especially in the decentralised web. By setting up honeypots that mimic different types of services and protocols, organisations can effectively detect and prevent illegal content, phishing attempts, and other malicious activities. Vetterl (2020) also mentioned that honeypots can be used to detect, track, and mitigate attacks, especially those that target the Internet of Things (IoT) devices. Deflandre (2022) further highlighted that honeypots can be used to study third-party application behaviour, and organisations can identify vulnerabilities and weaknesses that attackers can exploit. Lastly, Suroso and Prastya (2020) pointed out that honeypots can be used with Security Information and Event Management (SIEM) to enhance cybersecurity in higher education institutions.

In terms of effectiveness, research studies have shown that honeypots are an efficient tool in collecting threat intelligence, detecting and preventing illegal content, mitigating attacks, and improving cybersecurity. According to Mashima et al. (2020), honeypots are effective when they are designed to mimic specific systems or services that attackers are targeting. To keep up with evolving attacker tactics, honeypots should be dynamic and adaptive, with configurations changed frequently. Hassan et al. (2021) also highlighted that honeypots are effective in detecting and preventing illegal content in the decentralised web. For this purpose, honeypots should be designed to mimic different types of services and protocols, thereby detecting a broad range of attacks. Vetterl (2020) emphasised that honeypots are effective in detecting, tracking, and mitigating attacks, especially those targeting IoT devices. To enhance their effectiveness, honeypots should be integrated with other security tools such as firewalls and intrusion detection systems. Deflandre (2022) suggested that organisations should focus on creating high-interaction honeypots that can provide detailed information about attacker behaviour. Such honeypots are effective in studying third-party application behaviour, especially when they are designed to mimic specific application types. Lastly, Suroso and Prastya (2020) showed that honeypots, when used with SIEM, are effective in improving cybersecurity in higher education institutions by providing real-time monitoring and analysis of security events.

2.2 Benefits and Drawbacks of Using Honeypots as a Cybersecurity Measure

Honeypots can provide significant benefits for organisations seeking to enhance their cybersecurity posture. They can detect and prevent attacks, divert attackers from real systems, and educate security personnel. However, honeypots also have several drawbacks, including high deployment and maintenance costs, the potential to create a false sense of security, and legal and ethical concerns. Organisations must weigh the benefits and drawbacks of honeypots before deciding whether to deploy them as part of their cybersecurity strategy.

Benefits:

Organisations looking to bolster their cybersecurity defences can enjoy various advantages by implementing honeypots. Firstly, honeypots can serve as an early warning system, effectively detecting and preventing attacks. By deploying honeypots within a network, organisations can attract potential attackers and gather valuable intelligence on their methods and motivations. This information can then be used to improve the organisation’s overall cybersecurity posture. According to Amal and Venkadesh (2022), honeypots are especially useful in identifying new or unknown types of attacks, such as zero-day attacks, which may not be detected by traditional security measures.

Secondly, honeypots can help divert attackers from actual systems, reducing the risk of successful attacks. By redirecting attackers to honeypots, organisations can minimise the damage that may occur if real systems were compromised. Additionally, honeypots can be used to gather intelligence on the tactics, techniques, and

procedures (TTPs) used by attackers. This information can be used to improve incident response and forensic investigations.

Thirdly, honeypots can serve as educational tools for security personnel. By simulating real systems and monitoring the actions of attackers, security personnel can gain hands-on experience in identifying and responding to attacks. This can help organisations develop more effective security policies and procedures.

Drawbacks:

While honeypots offer a range of benefits, organisations should also be aware of their potential drawbacks. Firstly, honeypots can be expensive and time-consuming to deploy and maintain. They require significant resources to set up and configure, and they must be regularly updated to remain effective. According to Maesschalck et al. (2021), deploying and maintaining honeypots requires significant expertise, which can be challenging for organisations with limited IT resources.

Secondly, poorly designed or maintained honeypots can create a false sense of security, leaving real systems vulnerable to attacks. Attackers can easily identify and avoid honeypots that are not properly configured and monitored. It is therefore important for organisations to regularly test and update their honeypots to ensure their effectiveness.

Lastly, the use of honeypots can raise legal and ethical concerns, particularly if they are used to gather information about attackers without their consent. Organisations must ensure that their use of honeypots complies with relevant laws and regulations and does not violate the privacy rights of individuals or organisations.

2.3 Tactics, Techniques, and Procedures (TTPs) of Attackers

In cybersecurity, attackers use a range of tactics, techniques, and procedures (TTPs) to exploit vulnerabilities in computer networks, steal confidential information, and compromise critical systems. TTPs refer to the methods and procedures used by attackers to achieve their goals, which can include tactics like reconnaissance, exploitation, lateral movement, and exfiltration. As the cybersecurity landscape evolves, attackers continuously adapt their TTPs to bypass security defences, making it vital for organisations to understand these tactics to develop effective countermeasures.

Reconnaissance

One of the most critical TTPs employed by attackers is reconnaissance. Reconnaissance is the process of gathering information about a target network, including its topology, system configurations, and user credentials. Attackers use this information to identify potential vulnerabilities that they can exploit later in the attack. To study attackers' reconnaissance tactics, organisations can use honeypots. Honeypots are decoy systems that mimic vulnerable targets, and they can collect data on attackers' reconnaissance activities. This

information can help organisations gain valuable insights into attackers' tactics, enabling them to develop effective security defences.

Exploitation

Exploitation is another key TTP used by attackers to gain unauthorised access or control over computer systems. Attackers employ various techniques to exploit vulnerabilities, including buffer overflow attacks, SQL injection attacks, and cross-site scripting attacks. Like reconnaissance, honeypots can be used to study attackers' exploitation techniques. By mimicking vulnerable systems and observing attackers' activity, honeypots can provide valuable data on how attackers exploit vulnerabilities. Organisations can use this information to improve their security defences and protect their systems against potential attacks.

Lateral Movement

Lateral movement involves moving from one system to another within a network, often using compromised credentials. Attackers use this tactic to gain access to additional systems and further compromise the network. To study attackers' lateral movement techniques, organisations can use honeypots to create a realistic network environment. By observing attackers' behaviour in the honeypot environment, organisations can gain insights into their lateral movement techniques and use this information to develop effective countermeasures.

Exfiltration

Exfiltration refers to the process of stealing sensitive data from a network and transferring it to a remote location controlled by the attacker. Attackers use various techniques to exfiltrate data, such as using encrypted communication channels and obfuscating data to avoid detection. Honeypots can be used to study attackers' exfiltration techniques, as they can collect data on attackers' activity and provide valuable insights into their tactics. Organisations can use this information to develop effective countermeasures to prevent data exfiltration.

How Honeypots Help in Understanding TTPs:

Honeypots are an essential tool in understanding the tactics, techniques, and procedures (TTPs) utilised by attackers. These can be designed to mimic specific systems or applications, and hackers who target these systems or applications can be lured into the honeypot environment. By analysing the data collected from honeypots, organisations can gain valuable insights into the TTPs used by attackers and use this information to develop effective countermeasures. Also, honeypots are useful in collecting information about the different TTPs used by attackers, including reconnaissance, exploitation, lateral movement, and exfiltration techniques. The activity observed in the honeypot environment can provide valuable insights into the specific attack techniques used by attackers to exploit vulnerabilities in the target system or application.

For instance, a honeypot designed to mimic a vulnerable web application can provide valuable data on the specific attack techniques used by hackers to exploit vulnerabilities in the web application. This information can be used to develop effective countermeasures to prevent similar attacks from happening in the future. By

analysing the data collected from honeypots, organisations can develop effective security defences to prevent attacks that use similar TTPs. By identifying and analysing the TTPs used by attackers, organisations can gain a better understanding of the threats they face and develop effective security measures to mitigate them.

2.4 Challenges Associated with Implementing Honeypots with Traps and their Solutions

Implementing honeypots with traps can be challenging, but it is essential for detecting and preventing internal cyber-attacks. In this section, we'll discuss some of the challenges associated with the implementation of honeypots with traps and their potential solutions based on the literature.

Complexity: Setting up and maintaining honeypots with traps can be complex and require a significant amount of time and resources. This can be a barrier to entry for some organisations. To address this challenge, López-Morales et al. (2020) suggest using next-generation honeypots that integrate machine learning techniques to automate the configuration and maintenance of the honeypot.

Detection of False Positives: Honeypots with traps can generate a significant number of false positives, leading to unnecessary alarms and alert fatigue. To address this challenge, Tambe et al. (2019) propose the use of scalable VPN-forwarded honeypots that can generate a high volume of data while minimising false positives.

Detection of Advanced Persistent Threats (APTs): APTs are becoming increasingly sophisticated, making it challenging to detect them using conventional honeypots with traps. López-Morales et al. (2020) suggest that next-generation honeypots can use deep learning algorithms to detect APTs, which can significantly enhance their effectiveness.

Resource Utilisation: Honeypots with traps can consume significant amounts of system resources, making it challenging to deploy them on large-scale systems. To address this challenge, Parvathi (2021) suggests using virtual honeypots as they do not require physical hardware and can be deployed on existing infrastructure.

Security Risks: Honeypots with traps can also pose a security risk if they are not configured correctly. Attackers can exploit honeypots with traps and use them as a launching pad for attacks on real systems. To address this challenge, López-Morales et al. (2020) suggest using honeyplc, a next-generation honeypot that is specifically designed for industrial control systems and can detect attacks without posing a security risk.

Legal Issues: Implementing honeypots with traps can raise legal issues, especially if they capture sensitive data protected by privacy laws. Organisations need to consider legal issues when implementing honeypots with traps and ensure that they comply with relevant laws and regulations.

Cost: Implementing honeypots with traps can be costly, especially for small and medium-sized organisations. To address this challenge, Parvathi (2021) suggests using open-source honeypots that can help reduce the cost of implementing honeypots with traps while still providing effective security.

Lack of Expertise: Finally, implementing honeypots with traps can be challenging for organisations that lack the necessary expertise in cybersecurity. López-Morales et al. (2020) suggest that organisations can address this challenge by using managed honeypot services provided by cybersecurity experts.

2.5 Exploring Current Research Trends in Honeypots and Cybersecurity

Researchers are continually working on developing new techniques and strategies to enhance the effectiveness of honeypots. The latest research trends in honeypots and cybersecurity include the following:

Detecting Threats to IoT Devices: With the increasing number of devices connected to the internet, IoT security has become a crucial concern. Tambe et al. (2019) proposed a scalable VPN-forwarded honeypot system for detecting IoT device threats. The system was found to be effective in detecting different types of attacks on IoT devices. Such a system can be useful in protecting IoT devices and ensuring that attackers are detected before they can cause damage.

Deception-based Honeypots: Deception-based honeypots are a new generation of deception that software engineering teams can use to outwit attackers. Shortridge and Petrich (2021) proposed a deception environment that creates an illusion of a real system that attackers can interact with while recording their activities. By building such a deceptive environment, the system can gather valuable information on attacker behaviour and better prepare for future attacks.

Protecting Critical Infrastructure: Critical infrastructure protection is essential for cybersecurity. Barak (2020) studied a honeypot deployed to detect attacks on critical infrastructure. The study found that attackers tend to target infrastructure based on its perceived importance, but a honeypot can be used to deceive attackers and protect the real infrastructure. The study demonstrated that honeypots can be an effective means of protecting critical infrastructure.

Machine Learning: Machine learning is a vital tool in cybersecurity, and researchers are exploring its application in honeypots. Mekki et al. (2021) proposed a machine learning-based honeypot system for detecting malware attacks. The system used a combination of clustering algorithms and support vector machines to detect malicious activities. The study showed that machine learning can enhance the effectiveness of honeypots in detecting malware attacks.

Virtual Security: Virtual honeypots are cost-effective and easy to deploy, making them an attractive option for small and medium-sized businesses. Garcia et al. (2020) proposed a virtual honeypot system that uses artificial intelligence to simulate different types of attacks. The system was found to be effective in detecting various types of attacks.

Cloud Security: Cloud computing is gaining popularity, and cloud security is a critical concern. Varol et al. (2021) proposed a cloud-based honeypot system for detecting attacks on cloud infrastructure. The system was found to be effective in detecting various types of attacks on cloud infrastructure.

In conclusion, the effectiveness of honeypots is heavily reliant on the deployment strategies used. Researchers have explored various strategies for honeypot deployment, including active and passive deployment. Al-Akhras et al. (2020) proposed a hybrid honeypot deployment strategy that combines both active and passive honeypots to improve effectiveness. By keeping up with the latest research trends, organisations can better protect themselves against potential cybersecurity threats.

2.6 Best Practices for Implementing and Monitoring Honeypot Systems in Organizations

To effectively implement and monitor honeypot systems, organisations must follow best practices. As per literature review, the best practices for implementing and monitoring honeypot systems in organisations.

Define Objectives:

Before implementing a honeypot system, organisations need to define its objectives. The objectives could include gathering information about attacks, analysing attacker tactics, identifying vulnerabilities in the network, or acting as a deterrent. These objectives should align with the overall cybersecurity strategy of the organisation. Defining the objectives of the honeypot system will help organisations in selecting the right type of honeypot and in monitoring the system effectively.

Select the Right Type of Honeypot:

Choosing the right type of honeypot is critical for organisations to achieve their objectives, utilise their resources and expertise effectively. Different types of honeypots are available, including high-interaction, low-interaction, and hybrid honeypots. High-interaction honeypots provide more interaction between the attacker and the system but require more resources and expertise to maintain. Low-interaction honeypots provide limited interaction between the attacker and the system, but are less resource-intensive and easier to maintain. Hybrid honeypots combine the features of high-interaction and low-interaction honeypots. The right type of honeypot should align with the objectives, resources, and expertise of the organisation.

Proper Placement:

Honeypots need to be placed in the right place in the network based on their objectives and available resources. Placing honeypots in the internal network can help detect insider threats, while placing them outside the network can help detect external threats. Therefore, organisations should place the honeypot system in a location where it is most likely to attract attackers.

Use Deception Techniques:

Using deception techniques such as fake data, services, and vulnerabilities can make the honeypot system look real and attractive to attackers. Deception techniques can increase the chances of detecting attacks and should be used to make the honeypot system more effective.

Monitor Regularly:

Organisations ought to monitor the honeypot system regularly to detect any suspicious activity. Monitoring should include logging all activities, analysing logs, and generating alerts. Regular monitoring will help organisations detect attacks early and prevent future attacks.

Use Automated Tools:

Using automated tools can help organisations monitor their honeypot system effectively, analyse logs, generate alerts, and respond to attacks automatically. Automated tools can help organisations to scale their honeypot system and reduce the workload on security personnel.

Share Information:

Sharing information gathered from the honeypot system with other organisations and cybersecurity communities can help detect and prevent attacks, learn from each other, and improve honeypot systems.

Regularly Review and Update:

Organisations should regularly review and update their honeypot system to ensure its effectiveness. Regular reviews and updates should include checking the objectives, type of honeypot, placement, deception techniques, monitoring practices, and automated tools used. This will help organisations identify any weaknesses in their honeypot system and make necessary improvements.

2.7 New Contribution of this Study to Cybersecurity

According to Johnson (2019), researchers have explored the effectiveness of honeypots in detecting various types of attacks, including malware, ransomware, and phishing attacks. For instance, Tambe et al. (2019) proposed a scalable VPN-forwarded honeypot architecture to detect threats to IoT devices. They developed a method to detect and track attackers' behaviour and identify the type of attack being executed. Additionally, Shortridge and Petrich (2021) proposed a new generation of deception by creating deception environments to lure attackers away from real systems.

This study makes a new contribution to the field of cybersecurity by proposing the use of honeypots with traps to detect and prevent internal attacks. While Barak (2020) described how honeypots can be used to protect critical infrastructure by gathering intelligence on attackers' behaviour, this study extends the use of honeypots to detect internal attacks, where an insider may have access to the system and can cause damage. The honeypots with traps aim to attract internal attackers to a decoy system and monitor their behaviour to prevent damage to the actual system.

The traps used in the honeypots are designed to mimic the vulnerabilities and weaknesses of the real system, making it appear as a valuable target for an attacker. The honeypots can be customised to simulate different systems and applications, making it challenging for attackers to detect whether they are real or not. Once an attacker is detected, security experts can learn about the attacker's methods, motives, and prevent future attacks.

This new contribution to honeypots with traps is crucial because insider threats are becoming more prevalent in organisations. Insider threats can be difficult to detect as attackers may have access to the system and may not be detected by traditional security measures. By using honeypots with traps, security experts can detect insider threats and prevent damage to the system.

Chapter 2 Summary

Chapter 2 of the study delves into the historical background and development of honeypots, which can be traced back to the early days of the internet and the evolution of technology. The advantages and disadvantages of utilising honeypots as a cybersecurity measure are also thoroughly discussed. Honeypots offer benefits such as detecting attacks early and collecting information on attackers' tactics. However, organisations should be wary of potential drawbacks such as increasing the attack surface and the risk of false positives.

Furthermore, the chapter explores the tactics, techniques, and procedures (TTPs) employed by attackers, and how honeypots can help organisations in comprehending them. It also highlights the challenges associated with implementing honeypots with traps and proposes solutions to tackle them. The chapter concludes by examining the present trends in honeypots and cybersecurity research and providing best practices for setting up and monitoring honeypot systems in organisations. Additionally, the study's novel contribution to cybersecurity is emphasised, which includes an analysis of the effectiveness of honeypots in identifying and preventing attacks.

Chapter 3: Research Methodology

3.1 Research Design for the Project

The project utilised an experimental design as the research design. This design is most appropriate for investigating the effectiveness of honeypots with traps in preventing internal cyberattacks. According to Mohan et al. (2022), experimental designs provide a controlled environment, which is ideal for testing the hypothesis. The study aimed to test the hypothesis that honeypots with traps are effective in preventing internal cyberattacks. An experimental design enabled the manipulation of the independent variable, honeypots with traps, and the measurement of the effect on the dependent variable, internal cyberattacks (Shi et al., 2021). The study involved using honeypots with traps to detect and prevent internal cyberattacks. The honeypot simulated a vulnerable system that attackers could exploit to gain access to the organisation's network. Traps within the honeypot triggered an alert when an attacker attempted to access the system. The data collected from the honeypots were analysed to determine the effectiveness of the honeypots in preventing internal cyberattacks. The experiment was conducted in a controlled environment to eliminate the influence of extraneous variables.

The experimental design was ideal for the research study as it allowed testing the effectiveness of honeypots with traps in preventing internal cyberattacks. The controlled environment ensured that the results obtained were valid and reliable and that the experiment could be replicated in different settings. Honeypots with traps provided a practical and efficient solution for detecting and preventing internal cyberattacks. The experiment provided valuable insights into the effectiveness of honeypots in preventing internal cyberattacks. Additionally, the experimental design allowed the researcher to test different configurations of honeypots with traps and determine the optimal configuration for preventing internal cyberattacks. The study investigated the impact of different honeypot configurations on the number of internal cyberattacks detected and prevented. The results obtained from the experiment provided recommendations for the honeypots' optimal configuration to effectively prevent internal cyberattacks.

3.2 Data Collection Techniques Used in the Study

Data collection techniques refer to the methods used to gather and collect data for research purposes. Choosing the right data collection method is crucial as it can impact the quality and reliability of the data collected. The following data collection techniques were utilised in this research:

Literature Review

To gain a comprehensive understanding of honeypots and their effectiveness in preventing internal cyber-attacks, a systematic and extensive review of the existing literature on the topic was conducted. Relevant research articles, books, and other sources were searched using academic databases such as Google Scholar, IEEE, and Science Direct.

Scientific Publications

To obtain more in-depth information from cybersecurity professionals who have implemented honeypots in their organisations, scientific publications were utilized. The scientific publications aimed to collect information on the challenges and limitations of using honeypots, the effectiveness of honeypots in preventing internal cyber-attacks, and the factors that influenced the decision to implement honeypots.

Case Studies

Case studies were utilised to analyse the effectiveness of honeypots in preventing internal cyber-attacks. Organisations that have implemented honeypots as a preventive measure against internal cyber-attacks were studied to gather information on the implementation process, the benefits and limitations of using honeypots, and the factors that influenced the decision to implement honeypots.

The above data collection techniques were selected because they provided a comprehensive and in-depth understanding of honeypots and their effectiveness in preventing internal cyber-attacks. The literature review served as the theoretical foundation for the research, while the case studies provided practical insights into the use of honeypots in various organisations. By combining these data collection techniques, the researcher was able to collect reliable and valid data for the research.

3.3 Data Analysis Techniques

The study selected each of the following techniques based on its suitability in analysing the different types of data collected in the study.

The primary data analysis technique utilised in this research project was descriptive analysis. The researcher chose this method as it allowed for an effective description of the collected data. This method involved summarising and organising the data to gain insight into the patterns and characteristics that emerge from the data.

The next data analysis technique was content analysis, which was utilised to analyse data obtained from the literature review and case studies. This technique involved examining written materials such as articles, books, and reports to identify patterns, concepts, and themes. In this study, content analysis was used to identify various honeypot techniques used in preventing internal cyberattacks.

Statistical analysis was another data analysis technique used in this study. This method was employed to analyse the data collected through the case studies conducted in the study. Statistical analysis helped identify the relationships between the variables in the study, such as the effectiveness of honeypots in preventing internal cyberattacks.

The data collected through the case studies were analysed using a comparative analysis technique. This method helped compare the effectiveness of honeypots with traps in preventing internal cyberattacks across different organisations. Comparative analysis identified the similarities and differences between the various cases studied and their effectiveness in preventing internal cyberattacks.

Lastly, a qualitative analysis technique was employed to analyse the data collected through the research papers conducted in this study. Qualitative analysis helped to understand the meaning behind the responses and identified the perceptions and experiences of the research papers on the effectiveness of honeypots with traps in preventing internal cyberattacks.

3.4 Ethical Considerations in the Research Project

The importance of ethical considerations in research cannot be overstated. This research project has several ethical considerations that must be addressed, which are discussed below.

Risk to Users

The use of honeypots may inadvertently expose real system vulnerabilities, especially if traps are not correctly set up. This risk was minimised by utilising virtual honeypots in a controlled environment to decrease the likelihood of real-world attacks. It is crucial to consider the potential risks to users in any research project.

Data Storage

Data privacy is an ethical consideration when collecting and storing data in any research project (Huang et al., 2019.). The data collected during the research project was used exclusively for research purposes. The data was stored in a secure location, and access was restricted to authorised personnel only.

User Anonymity and Confidentiality

Participant anonymity and confidentiality are critical ethical considerations in any research project. To protect participants' identities, the data collected during the research project was anonymised. The data was stored in a secure location, and access was restricted to authorised personnel only.

Fair Use of Data

The ethical consideration of fair use of data ensures that the data collected during the research project is used solely for research purposes. As per Dowling, Schukat and Barrett (2020), any dissemination or publication of the data was done with the participant's consent and was conformed to ethical guidelines and principles.

3.5 Potential Limitations of Research Methodology

The research methodology employed a range of techniques including literature reviews and case studies. There are limitations associated with the data collection techniques used in this study. For example, the literature review may have been restricted by the availability of relevant sources. Additionally, the case study representativeness and accuracy may have been limited due to the sample size and response rate. Research papers may have also been restricted by participants' willingness to disclose information, and case studies may not be applicable to other settings. Therefore, acknowledging these limitations is crucial when interpreting the study's findings (Huang et al., 2019).

Limitations exist in the generalizability of research findings. Case studies, for instance, may not be relevant to other settings or apply to some populations. It is important for researchers to recognise that the findings may only be applicable to the specific context of the study. Moreover, the reliability of research findings may also be limited. Scientific publications, for example, may have experienced measurement error where participants may not have provided accurate responses. Similarly, observer bias may have influenced the interpretation of data in case studies. To address these limitations, researchers must standardise data collection methods and ensure systematic analysis. Doing so can reduce the impact of measurement error and observer bias on the results. As a result, the findings are more likely to be reliable and applicable to other settings or populations. As Franco et al. (2021) noted, researchers can improve the reliability of their findings by using standardised measures and procedures. Similarly, Ikuomenisan and Morgan (2022) emphasised the importance of triangulation - the use of multiple sources of data - to ensure the validity and reliability of research findings.

The research methodology may have been limited by time constraints, which could have made it difficult to conduct a comprehensive literature review and case studies. To overcome this limitation, the researcher should have prioritised the most relevant data collection techniques and ensured that the data collected was sufficient to answer the research questions.

The research methodology may have also been limited by resource constraints, such as limited funds or personnel. As a result, extensive papers and case studies may have been difficult to carry out. To address this limitation, the researcher should have focused on cost-effective data collection methods and utilised resources efficiently.

Ethical considerations may have been a limitation of the research methodology, particularly with regard to ensuring participant privacy and confidentiality during research. It was also important to obtain informed consent from participants before collecting data. To overcome this limitation, according to Nawrocki et al. (2023), the researcher should have ensured that the research was conducted ethically and responsibly.

3.6 Practical Implementation of Research

Implementing the study's findings into practice required the installation of a series of virtual honeypots and traps. In order to lure in hackers, the honeypots were set up to look and function like real systems and services. The honeypots' activity can be monitored for any harmful attempts thanks to the traps set up to catch and log them. In addition, the virtual space was designed to function like a networked real-world setting. Software and other methods were used to keep an eye on the honeypots and traps. Packet capture and logging utilities like SNORT and Syslog were used to keep tabs on network activity. Once the logs were studied, the attackers' methods and any unusual behavior could be determined. Finally, the analysis results were applied to locate and fix security holes in the interconnected system. In order to better understand how to use honeypots with traps for preventing internal attacks in cybersecurity, the research was put into practice.

3.7 Ensuring Reliability and Validity of Research Findings in Chapter 3

The research project implemented various measures to guarantee the reliability and validity of the results. These measures aimed to minimise the occurrence of bias and errors and guarantee that the findings accurately represented the subject under scrutiny.

As suggested by Williams (2022), the research project employed scientific publications, case studies, and literature reviews as data collection techniques to gather extensive and diverse data. The collected data was analysed through triangulation, which involved cross-checking the consistency and accuracy of the findings using multiple data sources and methods. This technique enhanced the validity of the research. Moreover, the research project used a mixed-methods approach to collect both qualitative and quantitative data. This method ensured that both subjective experiences and objective facts related to the subject were captured, thus enhancing the reliability of the findings.

The research project ensured the validity of the results by using purposive sampling. The participants were selected based on their knowledge about the subject under investigation, ensuring the relevance and informativeness of the collected data. Additionally, the research project adopted a rigorous data analysis process. The collected data underwent qualitative data analysis techniques such as coding, categorisation, thematic analysis, and content analysis, ensuring the accuracy and consistency of the results. Furthermore, the research project employed member checking by sharing the findings with the participants to verify the accuracy of the collected data. This approach enhanced the credibility of the findings, ensuring that the data accurately reflected the participants' experiences. Finally, the research project acknowledged potential sources of bias and took measures to mitigate them. For example, the research project ensured the anonymity of the participants to mitigate the potential for social desirability bias in the scientific publications data.

3.8 Steps for Developing the Honeypot Software Tool

Below is the process taken to construct and run the honeypot software tool:

i. **Install Python:** The software utility must be created using Python, an open-source programming language. Follow the installation instructions unique to your operating system to install the most recent version of Python by downloading it from the official Python website (https://www.python.org/).
ii. **Install Snort:** In the software tool, Snort, an open-source intrusion detection and prevention system, will be utilized. Follow the installation instructions provided when downloading Snort from the official Snort website (https://www.snort.org/).
iii. **Install Additional Python Libraries:** You might need to install more Python libraries, depending on the particular functionalities and specifications of your software tool. Installing libraries like pyvmomi or pyVBox, for instance, may be necessary if you intend to use virtualization technologies. Use the pip install library_name command to install these libraries using Python's package manager.

iv. **Write the Software Code:** Write the code for the software utility in a new Python script using a text editor or an integrated development environment (IDE). You would specify features for designing trap-filled honeypots, keeping an eye on the honeypot system, simulating assault scenarios, and gauging the tool's efficiency. You can use the code that was previously provided as a starting point and tweak it to suit your unique needs.

v. **Configure Honeypot and Trap Settings:** Define the options and configurations for the honeypots and traps in the program code. The kind of decoy system to be built, the way the trap behaves when an attacker is found, and any other pertinent settings unique to your implementation are all included in here.

vi. **Implement Real-time Monitoring:** Create the ability to maintain the honeypot system in real time. This entails gathering and studying pertinent logs, including logs of network traffic, system activity, and attacker activity. It's possible that you'll need to use programs like Snort to gather the required logs and evaluate them inside your software.

vii. **Set Up a Simulation Environment:** Utilize programs like VirtualBox or VMware to set up a virtualized simulation environment. Create virtual machines that replicate a true corporate network, complete with workstations, servers, and another network equipment. Set up the virtual machines' network settings to mirror the desired network topology.

viii. **Deploy the Honeypot System:** Within the simulation environment, deploy the honeypot system. This entails running the software program you created on virtual machines and configuring them to function as honeypots with traps.

ix. **Simulate Attack Scenarios:** To simulate multiple attack scenarios within the virtualized environment, use attack simulation tools such as Metasploit. During these simulations, keep an eye on the honeypot system's performance and collect essential data for analysis.

x. **Evaluate the Software Tool:** Create code or scripts to test the software tool's effectiveness. Compare the honeypot system's results against those of other existing security techniques, such as firewalls, intrusion detection systems, and anti-virus software. Examine the trap mechanisms' accuracy, the tool's capacity to identify and prevent assaults, and the tool's usability for system administrators.

xi. **Document and Refine:** Document the software tool's functions, configurations, and evaluation findings throughout the development process. Based on feedback and any discovered changes, refine the code, user interface, and overall implementation.

xii. **Prepare the Tool and Framework:** Assemble the software tool, as well as any supplementary recommendations, best practices, and metrics, into a full package for establishing honeypots with traps. Create documentation or user guides to go along with the tool and framework, detailing how to configure, deploy, and assess the honeypot system.

By following these instructions, one can develop and run the software tool, which allows system administrators to simply design and deploy honeypots with traps, monitor the honeypot system in real-time, simulate attack scenarios, and evaluate the tool's effectiveness.

Chapter 4: Framework

4.1 Best Practices for Configuring and Establishing Honeypots in Organizational Environments

The following are some best practices for setting up honeypots in a business setting:

First, establish the honeypot's purpose and aims. Before a honeypot can be setup and set up, its purpose and objectives must be defined. Honeypots can be used for several purposes, such as spying on hackers, learning more about them, and gauging the effectiveness of security measures. The purpose for which the honeypot is set up will determine the type of honeypot set up, where it is set up geographically, and what data is collected. The goals of the honeypot ought to be consistent with the broader organization security strategy.

Second, decide the honeypot setup you want to use, as each has its own set of advantages and disadvantages. While selecting honeypots, businesses should think carefully about their specific objectives. Low-interaction honeypots, for example, require little maintenance but provide no information on the tactics that hackers employ. Setting up and maintaining a high-interaction honeypot is more time-consuming than doing so with a low-interaction honeypot, but the insights gained into an attacker's methodology are invaluable.

Third, choose a spot for the honeypot, preferably one that is frequented by attackers but is physically isolated from the main network. This will prevent any potential threats from entering the manufacturing environment via the honeypot while still allowing the honeypot to gather and evaluate attacker activities.

Also, choose an OS and associated services: Businesses should go with a widely-supported OS and set of services. The honeypot's ability to lure in attackers will improve as a result of this improvement in realism. The attack surface and the possibility of introducing new vulnerabilities can be minimized by restricting the honeypot's emulation to only the most frequently attacked services.

The honeypot must be configured such that access is restricted, traffic is monitored, and information about attacker behaviour can be gathered. Only authorized users should be able to access the honeypot, and all outbound and incoming network traffic should be monitored by intrusion detection systems and packet sniffers. The attacker's methods, tools, and tactics, as well as any other relevant information, should be recorded by the honeypot.

The efficiency of the honeypot can be gauged by keeping track of attackers' actions, such as the quantity, types, origins, durations, and frequencies of attacks. This data can be used to strengthen the honeypot system and the company's overall security. Honeypots should be integrated with existing security infrastructure, including intrusion detection and prevention (IDP) and security information and event management (SIEM) systems. Because of the complexity of integration, experts may be needed. The effect of the honeypot system on production systems should be evaluated as a key indicator. The honeypot setup must have zero effect on live systems and must not introduce any new security holes.

Honeypots can create ethical and legal concerns, including data protection, privacy, and transparency, all of which should be addressed. Companies can solve these problems by taking precautions to safeguard honeypot data, collecting just the data absolutely necessary for analysis, being open about their honeypot practices, and adhering to all applicable laws and regulations.

Generally, honeypots are a useful tool for bolstering an organization's security posture; however, they require careful configuration and setup to prevent the introduction of new vulnerabilities, the waste of resources, and the increase of hazards. In order to strengthen their security, companies can benefit from using honeypots if they adhere to the best practices outlined in this article.

4.2 Integrating Honeypot System with Current Security Infrastructure

The project's honeypot software tool can be integrated into modern cyber-security frameworks with the right amount of planning and consideration of a number of factors. Honeypot software should be put in a central position where possible attackers can reach it quickly while still remaining isolated from the live system. As a result, the honeypot system will be less likely to be exploited by attackers looking for a route into the production network. It is advised that the honeypot system be connected to a separate network segment that is not connected to the production environment in order to monitor and analyse any traffic that may be flowing to or from the honeypot system.

The capacity to communicate and share data with other established security tools is also crucial. Using the honeypot with other security solutions like intrusion detection and security information and event management creates a more robust security infrastructure. This integration may be challenging and may call for specialized personnel, but it is essential for the proper functioning of the honeypot system.

The monitoring system's primary function is to document and analyse the adversary's actions in real time. The security team will be able to respond quickly and effectively if alerts are sent out whenever the monitoring system detects suspicious activity. Any attack on the honeypot system requires a well-thought-out response in order to contain the situation and prevent further damage. Stopping the attack, isolating the offender, or collecting evidence for later analysis are all options.

Data management is another crucial aspect to think about when combining the honeypot system with modern cybersecurity infrastructure. Large amounts of data can be generated by the honeypot system; proper data management is required for accurate evaluation of this data. Data management includes not just collecting information but also storing it, analysing it, and drawing conclusions from it. Tools like ELK Stack and Splunk can be used to analyse the honeypot system's data and help identify potential risks and their perpetrators.

Integration's maintenance method is also crucial. To ensure the continued functionality of honeypots, which are used to detect and probe intrusion attempts, routine maintenance is required. Updating software, fixing security holes, and checking logs are all part of routine maintenance. If the honeypot isn't updated often, it could

become obsolete and useless. So, it's crucial to assign workers with expertise in honeypot operation, maintenance, and tweaking.

4.3 Assessing the Efficacy of Honeypot Systems: Key Metrics to Consider

A honeypot system needs to be put through an efficiency test to ensure it is effective at catching intruders and preventing damage. When it comes to setting up honeypots with traps in businesses, this article will discuss the measures used to evaluate the efficacy of the suggested software solution.

The number of attacks is an important metric to consider when determining the efficiency of the honeypot system. The higher the number, the more interested attackers are, and the more effective the honeypot system has been at drawing them in. It is crucial to analyse the attack patterns and methods used by the attackers to gain a better knowledge of how effective the system is. Attack techniques including scanning, brute-force attacks, and vulnerability exploitation show that the honeypot system is a target for attackers. Failure to attract attackers could mean that the honeypot setup does not effectively replicate a vulnerable system.

The effectiveness of a honeypot system can also be gauged by looking at how long an attack lasts. If attacks last for less time, that could mean the honeypot is successful in deterring would-be hackers, while if they last longer, it could mean it isn't accurately simulating a vulnerable system. The duration of an attack might shed light on the assailants' motivation and the kind of the attack they are seeking to carry out.

The actions of those trying to breach the system are also a vital indicator of the honeypot's success in capturing and evaluating attacks. The attackers' methods, tools, and techniques, as well as any information gleaned from them, should be recorded and analysed by the honeypot system. This data can be used to strengthen the honeypot infrastructure and the company's security as a whole.

Maintenance is another important metric to use when determining the honeypot system's efficacy. After a honeypot has been set up, it requires regular upkeep to ensure it continues to function as intended in terms of detecting and analysing attacks. Updating software, fixing security holes, and checking logs are all part of routine maintenance. The honeypot will fast become useless if you don't keep up with maintenance.

Finally, another statistic that can be used to assess the efficiency of the honeypot system is how well it deals with data. When a honeypot is set up, it can generate a large amount of data on attackers' activities, such as the techniques, programs, and procedures they used. Storage, processing, and analysis of the honeypot's output data, as well as verification of the data's sufficient evaluation, are all essential components of efficient data management.

4.4 Potential Limitations and Challenges of the Framework Implementation

One potential drawback of using a honeypot system is the cost of implementation. It can be costly to set up and maintain a honeypot, especially one with a lot of moving parts and user involvement. The expensive initial investment in hardware, software, and personnel can make it difficult to roll out the honeypot system, which

can diminish its effectiveness. Businesses can get around this restriction by opting for low-interaction honeypots, which require less infrastructure, are cheaper to set up and maintain, and have a smaller impact on the environment.

Another possible drawback associated with honeypot usage is the difficulty of the implementation process. When using a highly interactive honeypot, it can be very challenging to decipher its workings. It can be challenging for businesses with limited resources and knowledge of computer security to set up and administer honeypots. To effectively fool attackers and record their actions, administrators must ensure that the honeypot is properly configured and maintained. So, it is crucial to go with a honeypot system that requires little in the way of setting and is easy to set up and manage.

When establishing a honeypot system, it is crucial to consider the ethical consideration of minimizing disturbance. While honeypots are effective at capturing the activity of attackers, they may negatively impact the user experience by interfering with the actions of legitimate users. On the other hand, improperly configured honeypots can inadvertently start an assault against the organization, causing unwanted damage. Businesses can lessen the chance of disruptions by setting up honeypots with low contact and no real services.

Another possible barrier is the risk of legal and ethical issues for businesses using honeypot technology. A honeypot can be used to entrap an attacker by luring them into attacking a vulnerable part of a system or network. Furthermore, honeypots can be used to illegally and inappropriately obtain private information like login credentials. Organizations should be aware of the legal and ethical concerns that honeypots bring and take precautions to ensure that their usage of honeypots is in accordance with all relevant laws and regulations.

Last but not least, there is also the issue of data handling while setting up honeypots. In order to conduct an accurate analysis of the honeypot system's output, proper data management is required. Data management includes not just collecting information but also storing it, analysing it, and drawing conclusions from it. Administrators must make sure they have the manpower and expertise to handle the influx of information generated by the honeypot.

4.5 Exploring the Ethical Considerations of Honeypot Deployment in Organizational Settings

The Honeynet Project's approach provides guidelines for the ethical use of honeypots in the workplace. This method places an emphasis on things like getting people's permission before doing anything, being as honest as possible, not causing too much trouble, keeping things running smoothly, according to the law, and so on.

Informed consent is the primary ethical consideration in the framework. Notifying and receiving permission from the intended audience is required for obtaining informed consent prior to deploying honeypots. The regulation stipulates that businesses must inform their staff, clients, and business associates of any honeypot installations.

Minimal deception is the second ethical consideration of the framework. Conceptually, honeypots shouldn't attempt to trick attackers into thinking they're dealing with a live system or network. Instead of actually offering services, honeypots should act like other systems or networks. Honeypots are recommended by the framework as a means for organizations to reduce fraud risk; these are low-engagement traps that do not provide any useful services.

The strategy takes care of the last ethical issue, which is data storage. Privacy rules may be broken if honeypots are used to collect information such as user names and passwords. The methodology suggests that businesses adopt measures like encryption and access controls to safeguard honeypot data. Businesses should only collect as much honeypot data as is absolutely necessary, according to the framework's recommendations.

The fourth ethical factor in the framework is minimizing disturbance. Honeypots can impede attacker operations, which may have an adverse effect on legitimate users. Honeypots with low levels of interaction and no real service delivery are recommended by the technique to help businesses mitigate service disruptions.

Fifthly, the framework places emphasis on maintaining a professional demeanour. This means that businesses employing honeypots have a responsibility to act in an ethical manner. The methodology suggests businesses employ honeypots with principles like honesty, integrity, and privacy protection in mind.

Transparency, the sixth element of ethics, is addressed by the framework. In order to build trust with their employees, customers, and partners, businesses must be transparent about their honeypot usage. Companies are encouraged to be transparent with their usage of honeypots by informing their staff, clients, and business partners. The guideline also suggests that businesses regularly report on their honeypot activity and the information they have gathered. Conformity with the law is the highest ethical priority in the framework. Honeypots must be used in accordance with all laws and regulations to ensure legal compliance. The recommendation of the guideline is that businesses follow privacy and data protection laws when setting up honeypots.

Chapter 5: Simulation and Evaluation

5.1 Simulation Environment Used to Evaluate the Software Tool

The simulation environment used to evaluate the honeypots with traps software was based on a model of the internet that was designed to mimic the structure of a real-world business network. Using virtualization software like VMware or VirtualBox, the virtual environment was built, allowing for the creation of several virtual computers that served as simulations of the various parts of a physical network. The parts included the servers, the workstations, and anything else connected to the network. The new features were tested in the virtual environment before being applied in the actual world. The honeypot system's effectiveness could be evaluated without jeopardizing any live systems because to the virtual environment's lack of danger and meticulous management.

To test the honeypot's efficacy, its designers created a simulated attack environment. The effectiveness of the honeypot system was measured by simulating numerous assaults, such as port scanning, attacks using brute force, and tapping into loopholes. Network traffic logs, systems log, and attacker activity logs all contributed to the massive amount of data produced by the simulated environment. ELK Stack and Splunk were used as data collection tools to gather these logs.

Honeypots with traps were set up with the help of the software application and monitored in real time to see if any suspicious behaviour arose during the simulated attack. Honeypots with traps may be set up and deployed with ease because to the tool's intuitive graphical user interface. Trap and decoy system types, as well as the trap's response when an intruder is spotted, could all be customized by the user. The software application tracked possible attacks on the honeypot system, recorded the attack's kind, origin, and whether or not the trap mechanism was successful in stopping the attack.

Most importantly, the research looked at how well the software tool could identify and prevent assaults, how well the trap mechanisms worked, and how easy it was to use for system administrators. Results from the audit were compared to other types of security measures, like firewalls, intrusion detection systems, and antivirus programs. The study evaluated honeypots with traps to find out how successful they are in preventing internal

cyber-attacks in businesses, and the tangible result of this research effort provided insights into the habits of cybercriminals. The research effort resulted in the creation of a software toolkit and a framework for building honeypots and traps in corporate settings.

5.2 The Different Attack Scenarios Simulated and How They Were Implemented

To determine if the honeypot system is effective at preventing internal cyberattacks, multiple simulated attack scenarios were run as part of the planned research project. These hypothetical intrusion attempts mimicked the most common tactics used by cybercriminals to breach a company's defences. Tools such as Metasploit, Nmap, and Wireshark were used to simulate attacks of varying complexity.

Among the many different kinds of attacks that were practiced here was the port scanning attack. One common method of reconnaissance used by attackers is to scan the network's ports in search of vulnerable systems. An adversary in this scenario used a port scanner, such as Nmap, to seek for vulnerable honeypot systems with open ports. This hypothetical attack scenario explains the attacker's triumphant course of action. The honeypot was programmed to detect such behaviour and respond with a trap, such as recording the attacker's IP address.

Simulated attacks were also used to train brute-force attacks. Brute-force attacks are a common way for an attacker to gain access to a system by guessing the correct password repeatedly until they succeed. The attacker in this case used a tool like Hydra to launch a brute-force attack against the honeypot system. The honeypot system was designed to detect such activity and immediately initiate a response, such as blocking the attacker's IP address.

Third, simulated attacks using phishing techniques were rehearsed. Social engineering assaults like phishing include tricking victims into giving up sensitive information like login credentials. The honeypot system was configured to look like a fake login page that otherwise functioned exactly like the genuine one, simulating a potential cyberattack. The honeypot system sprung its trap when an attacker tried to get in using the fake credentials, such as by logging the username and password. The attacker was thus unable to get any additional access to the system.

Finally, a malware attack simulation was run. Malware, short for malicious software, is software designed to steal information, sabotage systems, or gain unauthorized access to a computer. Malware is sometimes referred to as "spyware." The honeypot system was programmed to download and execute a sample of malicious software whenever an attacker attempted to download a bogus file. The honeypot infrastructure experienced this type of attack. The honeypot was programmed to detect such behaviour and respond with a trap, such as recording the attacker's IP address.

These made-up assaults were just examples of the numerous possible scenarios that may be simulated by the simulator. Using simulated attacks, researchers looked at how well the honeypot system protected against intrusion from within the network. The purpose of this was information gathering. The results of the simulations informed the development of a honeypot system with enhanced trap mechanisms, which would be used to prevent future cyberattacks from within the organization.

5.3 Key Metrics to Consider

The effectiveness of the honeypot software program at stopping attacks launched from within the company was evaluated based on several different parameters. The amount of attacks that were uncovered by the honeypot served as an early and crucial indicator. The number of attacks may provide some insight into the level of interest that the attackers have in the honeypot system as well as the level of success that the honeypot system has had in drawing them in. Analysing the attack patterns and methods utilized by hackers is another method that might be utilized to evaluate the efficiency of the honeypot system. Honeypot systems are a useful tool for preventing internal cyberattacks because they are designed to entice would-be hackers into a trap where they will be unable to escape. There are many different types of attack tactics, some examples of which include vulnerability exploits, scanning, and brute force attacks.

Additionally, resource use was monitored and recorded. The performance of the tool should not be negatively affected even if it forces the computer to consume an excessive amount of its resources, such as the central processing unit and random-access memory. It was required to compare the tool's resource consumption to that of other goods with a comparable function in order to determine whether or not it met acceptable standards. The

amount of time that passed after an attack was identified as such before a tool could respond to it might be referred to as the attack response time. Because of the decreased amount of time it took for the system to respond, it was able to limit the amount of damage caused by the assault.

The effectiveness of the honeypot system in capturing and analysing attacks was also evaluated by observing the behaviour of those who attempted to breach the system. The workflow of the attackers was captured and evaluated by the honeypot system, all the way down to the particular tools and strategies. This knowledge might be put to use to enhance not only the honeypot system but also the overall security measures taken by the firm. The application offered in-depth information regarding the nature of the attack as well as the TTPs (tactics, methods, and procedures) utilized by the opponent. The findings of the study offered a number of intriguing takeaways that can potentially be applied to the honeypot in order to make it even more successful.

In order to guarantee the program's reliability and efficiency in fighting against cyberattacks launched from within the company, its use by system administrators was also examined and reviewed. This was done to determine whether or not the program could successfully defend against attacks of this nature. Honeypots that were fitted with traps could be quickly and easily deployed by system administrators thanks to the software. The program also enabled real-time monitoring of the honeypot system, providing information about the number of attacks, the kind of attacks, and the locations from which the attacks originated.

5.4 Techniques Used to Evaluate Results of The Simulations

The simulated results were analysed using a number of different methods. First, the software tool's ability to detect and prevent threats was evaluated through analysis. The trap mechanisms' performance was assessed, and the mechanism's reaction to the presence of a possible threat was analysed. This helped determine how effective the honeypot system was in thwarting malicious insider attacks on the company's network.

The second factor that was analysed was how easy it was to use for system administrators. During testing, the software's efficacy, clarity, and user friendliness were assessed. This helped determine if the program was easy to navigate and provided system administrators with a practical solution.

Third, the simulation environment was evaluated based on its capacity to replicate a real-world business network. The network topology was checked against the organization's actual network infrastructure to ensure an accurate representation. This helped assess the veracity of the simulation's results by identifying whether or not they were similar to a real-world organizational network.

In the final stage, we looked at the amount of data the honeypot system generated to see if it was being handled well. Data management included actions like archiving, processing, and analysis. The information gathered by the honeypot system was accurately analysed, and new details about the attacker's actions emerged. The efficient administration of data allowed this to occur.

Finally, results from the examination were compared to those from other pre-existing security measures like firewalls, IDSs, and antivirus programs. This helped determine the honeypot system's viability in thwarting in-house intrusions.

5.5 Limitations and Errors in Simulation and Evaluation Methodology

The simulation setting may have some limitations in that it cannot perfectly imitate the conditions of a working business. This is a possible restriction. Assumptions and approximations form the basis of simulations, which means that attackers can behave differently in a simulated environment than they would in the actual world. This means that the simulation results could not reflect the results of the testing exactly.

One potential source of inaccuracy is the difficulty testers have in recreating real-world user behaviour. The accuracy of the evaluation results could be affected by how challenging it is to accurately duplicate legitimate user action in a simulated environment. The evaluation's results could be off if attackers figured out the simulated environment was a honeypot system and changed their attack strategies.

Furthermore, it is not clear what level of expertise the attackers who will be participating in the assessment will have. Inadequately skilled or unmotivated attackers in the simulation may lead to evaluation results that do not faithfully reflect the true effectiveness of the honeypot system. However, if the simulated attackers are very

skilled or motivated, the honeypot system may fail to thwart all of their attempts, leading to inaccurate assessments.

Finally, ethical concerns should be considered while using honeypots for research. It is crucial to adopt safety measures to guarantee that the honeypot system in the simulated environment will not endanger the legitimate users or systems. In addition, before doing any form of research, it is critical to be transparent and honest about the use of honeypots and to obtain the required ethical approval.

Chapter 6: Discussion and Conclusion

6.1 Key Findings and Analysis of the Cybersecurity Research Study

Key findings from the study include the fact that honeypots equipped with traps may effectively detect and thwart cyberattacks initiated from within an organization. Honeypots are a valuable instrument for obtaining information about possible attackers and their methods, tools, and reasons for launching assaults. The study concludes that honeypots are more enticing since they themselves are traps that resemble vulnerabilities or valuable assets. Information collected by honeypots can be effectively managed and analysed to reveal the level of the honeypot's success in thwarting internal cyberattacks. (Franco et al., 2021). The research also demonstrates the need for a system to deploy honeypots with traps in an organizational setting. The framework will offer direction for making the most of honeypots as a preventative strategy against internal cyberattacks. In addition to helping businesses operate ethically, this will ensure that honeypots and their data are managed properly.

The proposed research project plans to build a software instrument to deploy honeypots with traps and gain insights into the attackers' behaviour. The tool will also assess the effectiveness of honeypots as a deterrence against internal cyberattacks and report its findings. The study specifies the know-how and abilities needed to finish the study. Some examples of these are familiarity with cybersecurity fundamentals, networking, programming, virtualization, honeypot systems, data analysis, and research capabilities (Morishita et al.,2019). The investigation also reveals the means essential to the successful conclusion of the project. The report highlights these tools, which are mostly software-based and readily available through online resources. Study results suggest that using open-source software, virtualization technology, network gadgets, and data-gathering instruments would be useful to the project.

6.2 Implications of Research Project for Preventing Internal Cyber-Attacks in Organization

The outcomes of the cybersecurity research project, have substantial implications for the protection of businesses against insider cyberattacks. The planned study will investigate the efficacy of honeypots with traps in detecting and thwarting attacks before actual systems are compromised. Honeypots containing traps will be

set up for this purpose. In order to prevent internal attacks, the project proposes the development of a software application that, when implemented in enterprises, will enable the creation of honeypots with traps. The program would enable system administrators to select the type of trap to employ, the type of decoy system to construct, and the behaviour of the trap when an attacker is identified.

Using this application, the honeypot can be monitored in real time. The number of attacks, their nature, and their country of origin would all be monitored. Honeypots containing both honeypots and traps would be more effective at detecting and preventing attacks due to the fact that traps imitate vulnerabilities or valuable assets. The output of the tool would be actionable features that would assist businesses in bolstering their internal cybersecurity defensive mechanisms and protecting their digital assets from insider-launched intrusions.

The significance of this study lies in its proactive approach to detecting and mitigating intrusions. In light of the increasing threat posed by internal cyberattacks, there is a growing need for organizations to employ robust protection systems. This research methodology will evaluate the hypothesis that honeypots with integrated traps are an effective deterrent against insider cyberattacks against businesses. In addition, the study would investigate any potential limitations or obstacles related to its implementation.

In addition, the results of the study's practical component would contribute to the development of a deployment strategy for honeypots with traps within an organizational setting. This framework would instruct businesses on how to set up honeypots with devices to thwart internal cyberattacks. The framework would also specify the assets that businesses must possess in order to execute the process and manage the honeypot data effectively. Investigations into honeypots have focused primarily on their capacity to detect external intrusions. The proposed research would fill a gap in the existing literature and cast light on the potential utility of honeypots with traps in preventing internal cyberattacks.

6.3 Limitations and Future Directions for Research

Businesses are increasingly spending money on preventative steps to reduce the likelihood that attacks may originate within their own systems as the cybersecurity threat increases. Honeypots, which include traps, are

one such method. However, there could be a number of obstacles and complications in setting up such honeypots.

The use of honeypots and traps is problematic due to the possibility of false positives. Since honeypots are intended to seem like real systems, they can be triggered by accident by authorized users on the inside. False positive warnings may be created, and legitimate users may be denied access to resources. More advanced machine learning and artificial intelligence techniques can be tested in future studies to accurately differentiate between legitimate and malicious behaviour. The restriction's negative impact will be lessened.

Another disadvantage is the higher price tag associated with setting up a system that employs both honeypots and traps. Depending on the scale of the company, honeypot deployment and management can require a significant amount of time and manpower. However, it may be difficult to persuade higher management, especially in smaller businesses and organizations, to spend money on such cutting-edge technology. Future research may concentrate on developing low-cost honeypot systems, such as cloud-based honeypots, which would lessen the financial strain of establishing such a system.

Honeypots that include traps may be more or less successful depending on the attacker's skill level. A very adept attacker might know to just ignore the honeypot and go straight for the main target. Future research should focus on strengthening honeypots so that they can better withstand attacks from sophisticated, well-informed adversaries. Researchers, for instance, could hone decoy systems and trap mechanisms in an effort to fool and ensnare increasingly sophisticated adversaries.

Ethical concerns are another fallout from utilizing honeypots and traps. While honeypots are effective at revealing attacker habits, they have been called unethical due to the risk of compromising legitimate users' accounts. This paves the path for further research into methods for legally deploying honeypots in commercial settings. Methods in this category include the formulation of clear policies and procedures for the use of honeypots, as well as consistent communication with stakeholders about the implementation and purpose of honeypots.

6.4 Improving the Software Tool and Framework to Prevent Internal Cyber-Attacks in Organizations

Adding more sophisticated analytics tools to the honeypot software product is one method to improve it. Since it is hoped that the software tool would reveal information about the methods employed by attackers, it is crucial that the data collected from honeypots and traps be carefully analysed. Data anomalies and patterns can be uncovered with the use of advanced analytics tools, which can then be leveraged to strengthen security and foil attacks. Machine learning algorithms and anomaly detection methods are two types of the advanced analytics capabilities. For instance, the program may instantly and automatically terminate any suspicious network traffic by employing machine learning methods. Honeypots with this capability will be more effective and valuable since they can anticipate and stop attacks before they happen (Maesschalck et al., 2022). The software tool could be improved in other ways as well, one being the incorporation of extra security measures. While honeypots with built-in traps can help identify and thwart attacks, they are not infallible. Since attackers can learn to avoid these measures, it's crucial to put in place additional safeguards just in case. For instance, the program can be added to intrusion prevention systems (IPS) and firewalls to increase the protection that honeypots provide. Thus, the software solution can protect the company from any angle and effectively deter any potential dangers.

Adding more specific instructions for how to set up honeypots with traps is another way the framework might be improved. The framework must offer comprehensive instructions for setting up the honeypot's many parameters, such as its trapping methods, decoy systems, and subsequent behaviour upon detection of an intruder. In addition, the framework needs to provide advice on how to most successfully integrate the honeypot system with the existing security architecture at the organization. The extensive instructions for setting up honeypots and deploying them later are just two examples of how the framework may help businesses improve the efficiency and effectiveness of their honeypot system implementation.

The framework could also be improved by including more information about the legal and ethical problems that arise when using honeypots in a business setting. When companies deploy honeypots that contain traps to fool would-be attackers, ethical and legal questions arise over the practice. The framework should provide guidance on ethical honeypot use and ensure that the company is not breaking any laws or regulations by employing

them. In addition, the framework needs to incorporate rules for maintaining openness when reporting honeypot and trap use to key audiences like employees, customers, and business partners (Amal and Venkadesh, 2022). Finally, the effectiveness of the framework may be improved by providing a clear and succinct set of metrics with which to measure the honeypot system's performance. Metrics should reflect the security objectives of the organization and provide information about the number and type of attacks that were blocked by the honeypots. In addition, the metrics should shed light on the effectiveness of the techniques employed to catch attackers, as well as the trap's response once an intruder has been located. The framework provides a transparent set of indicators that may be used to measure the return on investment for deploying honeypots with traps and enhancing the honeypot system.

In conclusion, the research project on preventative internal attacks using honeypots with traps in cybersecurity can be enhanced by including more sophisticated analytic capabilities, including additional security mechanisms, providing more detailed guidelines for setting up and deploying honeypots, providing insights into the legal and ethical considerations of deploying honeypots, and providing a clear and concise set of metrics to evaluate the effective implementation of honeypots. The software tool and framework developed by the project to prevent insider cyberattacks could be made more effective with these modifications.

Reference List

AlZoubi, W. and Alrashdan, M., 2022. The effect of using honeypot network on system security. *International Journal of Data and Network Science*, *6*(4), pp.1413-1418. http://growingscience.com/ijds/Vol6/ijdns_2022_71.pdf

Amal, M.R. and Venkadesh, P., 2022. Review of cyber attack detection: Honeypot system. *Webology*, *19*(1), pp.5497-5514. https://www.webology.org/data-cms/articles/20220123051035pmWEB19370.pdf

Amal, M.R. and Venkadesh, P., 2022. Review of cyber-attack detection: Honeypot system. *Webology*, *19*(1), pp.5497-5514. https://www.webology.org/data-cms/articles/20220123051035pmWEB19370.pdf

Antonakakis, M., Perdisci, R., & Vasiloglou II, N. (2011). Detecting malware propagation through honeyclients. IEEE Transactions on Dependable and Secure Computing, 8(2), 223-235. https://doi.org/10.1109/TDSC.2009.28

Barak, I., 2020. Critical infrastructure under attack: lessons from a honeypot. *Network Security*, *2020*(9), pp.16-17. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7508537/

Casola, V., D'Antonio, S., and Romano, L. (2012). Building honeypots for detecting insider attacks in critical infrastructures. Computers and Security, 31(1), 1-17. https://doi.org/10.1016/j.cose.2011.08.004

Deflandre, G., 2022. Master thesis: Honeypot Evolution: Creation Guidelines and Implementation for Third-Party Application Behavior Study Using Cisco SecureX as Monitoring Toolkit. https://matheo.uliege.be/bitstream/2268.2/14580/5/Guilian%20Deflandre%20-%20Master%20Thesis%20-%20Honeypot%20Evolution%2C%20Creation%20Guidelines%20and%20Implementation%20for%20Third-Party%20Application%20Behavior%20Study%20Using%20Cisco%20SecureX%20as%20Monitoring%20Toolkit%20-%20Text%20Only.pdf

Dornseif, M., and Schreiber, T. (2005). Honeyd2–a virtual honeypot daemon. In Proceedings of the 2005 ACM Workshop on Rapid Malcode (pp. 33-41). https://doi.org/10.1145/1102120.1102127

Dowling, S., Schukat, M. and Barrett, E., 2020. New framework for adaptive and agile honeypots. *Etri Journal*, *42*(6), pp.965-975. https://onlinelibrary.wiley.com/doi/pdfdirect/10.4218/etrij.2019-0155

Franco, J., Aris, A., Canberk, B. and Uluagac, A.S., 2021. A survey of honeypots and honeynets for internet of things, industrial internet of things, and cyber-physical systems. *IEEE Communications Surveys & Tutorials*, *23*(4), pp.2351-2383. https://arxiv.org/pdf/2108.02287

Franco, J., Aris, A., Canberk, B. and Uluagac, A.S., 2021. A survey of honeypots and honeynets for internet of things, industrial internet of things, and cyber-physical systems. *IEEE Communications Surveys & Tutorials*, *23*(4), pp.2351-2383. https://arxiv.org/pdf/2108.02287

Gharib, S., Slay, J., and Moustafa, N. (2020). A survey of honeypot technology: Applications, challenges, and opportunities. Journal of Network and Computer Applications, 149, 102483. https://doi.org/10.1016/j.jnca.2020.102483

Hassan, A.I., Raman, A., Castro, I., Zia, H.B., De Cristofaro, E., Sastry, N. and Tyson, G., 2021, December. Exploring content moderation in the decentralised web: The pleroma case. In *Proceedings of the 17th International Conference on emerging Networking EXperiments and Technologies* (pp. 328-335). https://arxiv.org/pdf/2110.13500

Huang, C., Han, J., Zhang, X. and Liu, J., 2019. Automatic identification of honeypot server using machine learning techniques. *Security and Communication Networks*, *2019*, pp.1-8. https://www.hindawi.com/journals/scn/2019/2627608/abs/

Ikuomenisan, G. and Morgan, Y., 2022. Meta-Review of Recent and Landmark Honeypot Research and Surveys. *Journal of Information Security*, *13*(4), pp.181-209. https://www.scirp.org/journal/paperinformation.aspx?paperid=119340

Johnson, E.P., 2019. Honeypot. In *Honeypot*. Duke University Press. https://www.dukeupress.edu/Assets/PubMaterials/978-1-4780-0653-4_601.pdf

KOLAWOLE, A., 2019. NETWORK SECURITY USING HONEYPOT. http://ir.mtu.edu.ng/jspui/bitstream/123456789/139/1/AYANFE%20body%20of%20work.pdf

Korchenko, A., Breslavskyi, V., Yevseiev, S., Zhumangalieva, N., Zvarych, A., Kurchenko, O., Laptiev, O. and Tkachuk, S., 2021. Development of a method for constructing linguistic standards for multi-criteria assessment of honeypot efficiency. http://repository.hneu.edu.ua/jspui/bitstream/123456789/25618/3/Y%20e%20v%20s%20e%20i%20e%20v.pdf

Li, H. and Ren, J., 2022. A Novel Worm Propagation Model Considering the Connected State and Trap Mechanism of a Honeypot. *Engineering Letters*, *30*(4). https://www.engineeringletters.com/issues_v30/issue_4/EL_30_4_16.pdf

Liu, I.H., Lin, J.H., Lai, H.Y. and Li, J.S., 2022. Scalable ICS Honeypot Design by Description Files. *Journal of Robotics, Networking and Artificial Life*, *9*(3), pp.216-220. https://www.jstage.jst.go.jp/article/jrnal/9/3/9_2/_pdf

López-Morales, E., Rubio-Medrano, C., Doupé, A., Shoshitaishvili, Y., Wang, R., Bao, T. and Ahn, G.J., 2020, October. Honeyplc: A next-generation honeypot for industrial control systems. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security* (pp. 279-291). https://dl.acm.org/doi/pdf/10.1145/3372297.3423356

Maesschalck, S., Giotsas, V., Green, B. and Race, N., 2021. Don't get stung, cover your ICS in honey: How do honeypots fit within industrial control system security. *Computers & Security*, p.102598. https://www.sciencedirect.com/science/article/pii/S0167404821004211

Maesschalck, S., Giotsas, V., Green, B. and Race, N., 2022. Don't get stung, cover your ICS in honey: How do honeypots fit within industrial control system security. *Computers & Security*, *114*, p.102598. https://www.sciencedirect.com/science/article/pii/S0167404821004211

Mashima, D., Kok, D., Lin, W., Hazwan, M. and Cheng, A., 2020, August. On Design and Enhancement of Smart Grid Honeypot System for Practical Collection of Threat Intelligence. In *CSET@ USENIX Security Symposium*. https://www.usenix.org/system/files/cset20-paper-mashima.pdf

Mayorga, F., Vargas, J., Álvarez, E. and Martinez, H.D., 2019, November. Honeypot network configuration through cyberattack patterns. In *2019 International Conference on Information Systems and Computer Science (INCISCOS)* (pp. 150-155). IEEE. https://doi.org/10.1109/INCISCOS49368.2019.00032

Mohan, P.V., Dixit, S., Gyaneshwar, A., Chadha, U., Srinivasan, K. and Seo, J.T., 2022. Leveraging computational intelligence techniques for defensive deception: a review, recent advances, open problems and future directions. *Sensors*, *22*(6), p.2194. https://www.mdpi.com/1424-8220/22/6/2194/pdf

Morishita, S., Hoizumi, T., Ueno, W., Tanabe, R., Gañán, C., van Eeten, M.J., Yoshioka, K. and Matsumoto, T., 2019, April. Detect me if you… oh wait. An internet-wide view of self-revealing honeypots. In *2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)* (pp. 134-143). IEEE. https://pure.tudelft.nl/ws/files/51833538/IM2019_honeypot.pdf

Moustafa, N., and Slay, J. (2016). The effectiveness of honeypots as a proactive mechanism. Computers & Security, 59, 126-141. https://doi.org/10.1016/j.cose.2016.02.004

Nawrocki, M., Kristoff, J., Hiesgen, R., Kanich, C., Schmidt, T.C. and Wählisch, M., 2023. SoK: A Data-driven View on Methods to Detect Reflective Amplification DDoS Attacks Using Honeypots. *arXiv preprint arXiv:2302.04614*. https://arxiv.org/pdf/2302.04614

Nsiah-Konandu, A., Adu-Boahene, C. and Nikoi, S.N., 2022. Enhancing the Design of a Secured Campus Network using Demilitarized Zone and Honeypot at Uew-kumasi Campus. *Asian Journal of Research in Computer Science*, pp.14-28. http://eprints.asianrepository.com/id/eprint/2605/1/30304-Article%20Text-56755-1-10-20220216.pdf

Parvathi, P., 2021. A Honey pot Implementation for security Enhancement in IOT System using AES and Key management. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(3), pp.5206-5214. https://www.turcomat.org/index.php/turkbilmat/article/download/2149/1870

Pellegrino, G., Giacinto, G., and Sansone, C. (2010). On the effectiveness of low-interaction honeypots for malware collection. Journal of Computer Virology and Hacking Techniques, 6(4), 223-233. https://doi.org/10.1007/s11416-010-0134-4

Rajaboyevich, G.S., Rustamovna, S.H. and Azimjon o'g'li, B.S., 2022. Integrated Intrusion Detection and Prevention System with Honeypot on Cloud Computing Environment. *American Journal of Social and Humanitarian Research*, *3*(5), pp.266-270. https://www.globalresearchnetwork.us/index.php/ajshr/article/download/1118/1037

Sarfaraz, A., Jha, A., Mondal, A. and Goswami, R.T., 2022. An Efficient Detection and Prevention Approach of Unknown Malicious Attack: A Novel Honeypot Approach. In *Cyber Security and Digital Forensics: Proceedings of ICCSDF 2021* (pp. 11-19). Springer Singapore. https://doi.org/10.1007/978-981-16-3961-6_2

Shi, L., Wang, X. and Hou, H., 2021. Research on optimisation of array honeypot defense strategies based on evolutionary game theory. *Mathematics*, *9*(8), p.805. https://www.mdpi.com/2227-7390/9/8/805/htm

Shortridge, K. and Petrich, R., 2021. Lamboozling Attackers: A New Generation of Deception: Software engineering teams can exploit attackers' human nature by building deception environments. *Queue*, *19*(5), pp.26-59. https://dl.acm.org/doi/pdf/10.1145/3494834.3494836

Spitzner, L. (2003). Honeypots: catching the insider threat. Network Security, 2003(4), 10-14. https://doi.org/10.1016/s1353-4858(03)00065-5

Suroso, J.S. and Prastya, C.P., 2020, June. Cyber Security System With SIEM And Honeypot In Higher Education. In *IOP Conference Series: Materials Science and Engineering* (Vol. 874, No. 1, p. 012008). IOP Publishing. https://www.researchgate.net/profile/Jose-Benitez-Andrades/publication/341995239_Analyzing_IoT-Based_Botnet_Malware_Activity_with_Distributed_Low_Interaction_Honeypots/links/62519dd2ef0134206664d6fe/Analyzing-IoT-Based-Botnet-Malware-Activity-with-Distributed-Low-Interaction-Honeypots.pdf

Tambe, A., Aung, Y.L., Sridharan, R., Ochoa, M., Tippenhauer, N.O., Shabtai, A. and Elovici, Y., 2019, March. Detection of threats to IoT devices using scalable VPN-forwarded honeypots. In *Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy* (pp. 85-96). https://publications.cispa.saarland/2787/1/_CODASPY_19__Detection_of_Threats_to_IoT_Devices_using_Scalable_VPN_forwarded_Honeypots.pdf

Vetterl, A., 2020. *Honeypots in the age of universal attacks and the Internet of Things* (Doctoral dissertation, University of Cambridge). https://www.repository.cam.ac.uk/bitstream/handle/1810/303171/vetterl-thesis.pdf?sequence=1

Williams, R.T., 2022. Research Methods In Education: A Book Review. *European Journal of Education Studies*, *9*(11). https://oapub.org/edu/index.php/ejes/article/download/4582/7217

Zymberi, I., 2021. Honeypots: A Means of Sensitizing Awareness of Cybersecurity Concerns. https://www.theseus.fi/bitstream/handle/10024/496070/Zymberi_Ilirjana.pdf?sequence=