Implementation and Effectiveness of Honeypots in Modern Network Security Architecture

Vignesh Goud Badagouni

Webster University

Practical Research in Cybersecurity – CSSS 6000 Y3

Dr. Adewale Ashogbon

12-14-2025

INTRODUCTION

1.1 Background of The Study

Cybersecurity is now a top priority for Information Technology (IT), as the rapid evolution of the Internet, Cloud Computing, and device interconnectivity has created both enormous opportunities and significant risks. As a result of this trend, cyber-attacks such as Phishing, Ransomware, Denial-of-Service (DoS), and Data Breaches have grown in scale and complexity. All organizations in all sectors are under continuous threat of disruption to business operations, breach of sensitive data, and financial or reputational loss; therefore, effective defensive measures must be a component of every Network Security Architecture.

Honeypots, an increasingly effective form of protection against cyber-attacks, are now being deployed globally. Honeypots are decoy systems or servers that mimic network resources or services to attract hackers into interacting with them. Once a hacker interacts with a honeypot, security professionals can monitor their behavior, gather information on emerging hacking tactics, and improve their defenses. The idea behind honeypots was first developed in early systems used for intrusion detection but has evolved into a more advanced method of proactive cyber defense through the increasing use of AI and automation in cyber offense and defense.

The ongoing and increasing complexity of cyber-attacks represents a compelling reason to investigate ways to detect, deceive, and analyze potential hackers before they cause any damage to an organization's network or systems.

1.2 Statement of The Problem

Although honeypots are becoming increasingly popular among cybersecurity researchers and enterprises, they remain limited in application due to an incomplete understanding of their usefulness and their integration with current network architecture. In addition to attracting attackers and providing useful intelligence, honeypots require correct placement, maintenance, and protection from exploitation by adversaries.

In addition, most of the literature on honeypots has focused on their theoretical advantages rather than on empirical evidence of their effectiveness in real-world environments. From a theoretical perspective, the problem is also related to the changing nature of deception technology as it applies to cyber threats. Honeypots need to keep pace with new attack types, including automated botnets and AI-based exploits. This study was undertaken to close the gap by assessing how honeypots can be successfully incorporated into today's complex network environment and their contribution to the overall security posture of those networks.

1.3 Research Questions/Hypotheses

This study is structured around the following questions:

1. How may honeypot technology best be applied as a component of contemporary network security architectures?
2. Which of the three basic honeypot configurations (low-interaction, high-interaction, and hybrid) provide the greatest potential for identifying and analyzing intrusions into computer networks?
3. How much does the application of honeypot technology enhance a company's ability to detect threats, respond to them, and gather intelligence on attackers?
4. What are some of the limitations, challenges, and risks inherent in applying honeypot technology in operational networks?

The following hypothesis is based upon the above questions.

H_1: Honeypots provide substantial enhancements to both the detection of network intrusions and the subsequent analysis of those threats when deployed as part of contemporary network security architectures.

1.4 Objectives of The Study

The development of a plan to assess the operation of honeypots as an element of modern network defense systems.

Objectives:

1. To find out about the variety of honeypot types and setups that are relevant in today's networked world.
2. To examine the part played by honeypots in identifying and evaluating the nature of cyber threats.
3. To measure the impact of honeypots on improving the overall safety of a network and its ability to respond to incidents.
4. To consider the obstacles, hazards, and limitations related to the use of honeypots in a real-world environment.

1.5 Significance of The Study

Both Theoretical and practical contributions are present in this study.

Academically, this research is part of a developing collection of papers on cyber deception technology and its use in Proactive Security Strategies. Using a Structured Research Framework to analyze honeypots assists in understanding the ways deception based mechanisms may supplement traditional detection mechanisms such as Firewalls, Intrusion Detection Systems (IDS), and Security Information and Event Management (SIEM) tools.

For Practitioners and Cybersecurity Professionals, the results of this research may serve as a decision-making tool for designing networks, monitoring them, and mitigating threats to those networks. Policymakers and Institutional Leaders may also derive value from understanding how honeypot technologies help build organizational cybersecurity resiliency. By establishing Best Practices and Guidelines for deploying Honeypots ethically and legally, policymakers and institutional leaders can ensure compliance with Data Protection Regulations and maximize the potential benefits to research and defense.

1.6 Scope and Delimitation of the Study

The purpose of this study was to examine the implementation and functionality of honeypots in today's network security environment. This study focused on a specific type of honeypot (software-based) within an organizational/institutional network, rather than a larger-scale industrial/national cybersecurity system.

This study did not involve developing a comprehensive framework for commercially developed honeypots or conducting a forensic legal analysis of the data collected by honeypots. Instead, this study evaluated the practicality of using honeypots, focusing on their ethical performance. These limitations provided the necessary constraints to keep the researcher focused on the research objectives and to complete the study within the academic program's time frame.

1.7 Limitations of the study

As with any research project, this study has some limitations. The two main limitations are a lack of empirical data, because honeypots can be deployed to capture sensitive security data; therefore, organizations do not typically make public how they deploy them.

Technical issues that could impact the ability to develop an experimental setup include the quality and quantity of hardware, the quality of network infrastructure, and resource (financial) limitations. To minimize the negative effects of these limitations, the research will use controlled simulations, open-source honeypot platforms, and, secondarily, data from credible cybersecurity-related entities.

1.8 Definition of key terms

- Decoy Computer (honeypot): A computer designed to capture a malicious hacker, then log all of the actions they perform on the decoy.
- Misdirection/Deception in Cybersecurity: The use of misdirection to confuse an attacker while protecting your true resources.
- Architecture of Network Security: A conceptual model of how you will design and implement your security controls and devices to protect both your network and data.
- Intrusion Detection Systems: An IDS is a tool used by companies to monitor unusual patterns of network access.

1.9 Organization of the study

This research is structured into five chapters to show a clear, coherent progression through the different stages of the research process and its results.

Chapter One – Introduction

This Chapter provides an introduction to the research, including background information, the problem this research aims to address, research questions, objectives, relevance/significance, boundaries/limitations, and definitions of key terms.

Chapter Two - Literature Review

This Chapter reviews the current academic literature, scholarly articles, and prior research on honeypots, cyber deception techniques, and network security models/frameworks. This review will identify theoretical underpinnings, highlight gaps in the literature, and support the conceptual framework of this study.

Chapter Three - Research Methodology

This Chapter outlines the methodology employed in the study, including research design, data collection methods, population and sample size, research tools/instruments, and data analysis procedures. This Chapter ensures that the research methodology adopted is consistent with good practice, ethically defensible, and methodologically rigorous.

Chapter Four - Analysis and Interpretation

This Chapter presents and explains the data collected during the research. In addition to presenting the research findings, it will explain them in relation to the study's stated objectives and examine how honeypot implementations can contribute to the detection of intrusions, the identification of threats, and the overall effectiveness of network defense mechanisms.

Chapter Five - Conclusions and Recommendations

In the final Chapter, the main findings from the research are summarized and conclusions drawn from the analysis. Recommendations are made for organizations, policy makers, and other potential researchers. Finally, suggestions are provided for further research on honeypot technology and its growing importance in computer security.

LITERATURE REVIEW

2.1 Introduction

This chapter examines the existing literature on the application and efficacy of honeypots in current network security architectures. The goal of this review is to identify important theories, conceptual models, and empirical studies that demonstrate the contributions of honeypots toward enhancing network security defenses. This review will identify current knowledge gaps and outline how the present study will address some of them.

A literature review is an integration of prior research to clarify what has been learned, what has not yet been learned, and how further research may build upon previous findings. As such, the structure of this chapter includes a review of both theoretical/conceptual models, a thematic review of literature, synthesis, and identification of research gaps. Peer-reviewed journal articles, Cybersecurity Standards, and authoritative texts published between 2015 and 2024 were among the sources used for selection.

2.2 Theoretical Framework

Deception Theory provides a foundational base for D**eception-based systems** and H**oneypot development.** As defined by Rowe and Rushi (2016), Deception Theory states that creating false targets can enhance the effectiveness of security systems, which will ultimately create a barrier between an attacker's ability to carry out their attack plan, while exposing the attacker's behavior at the same time.

Deception Theory has been operationalized through the use of honeypots, which simulate vulnerable systems indistinguishable to attackers from "real" systems. The purpose of these systems is to enable defenders to monitor intrusion techniques in real time (Naeem, 2021). The Deception Theory model provides insight into the psychological and strategic aspects of cybersecurity as it allows defenders to manipulate an attacker's perceptions of a system to further defensive objectives.

The IDRF model was developed to support structured monitoring, detection, and mitigation of unauthorized access to computer systems. As described by Stallings (2021), honeypots can serve as integral components of an IDRF-based architecture, providing early alerts of malicious activity. In addition, honeypots provide information on previously unseen or unknown attack types, thereby providing organizations with additional threat intelligence. Hence, integrating honeypots into an IDRF-based architecture can help provide organizations with layered defenses.

2.3 Conceptual Framework

This Study's Conceptual Framework Relates Theoretical Constructs to Measurable Research Constructs. As part of a larger Defense-In-Depth Architecture, it views Honeypots as Proactive Elements of a Network Security Solution that will include Firewalls, SIEM Systems, IPS, and Other Solutions.

The Framework identifies three Major Constructs:

Implementation Strategy - Methods and Architectures Used to Deploy Honeypots (High vs Low Interaction Models).

Detection Effectiveness - Ability of Honeypots to Identify Attacks, Capture Attack Data, and Provide Situational Awareness.

Security Outcomes - Quantifiable Improvements in Network Defense (Fewer Breaches & More Threat Intelligence).

The conceptual model assumes that an effective implementation strategy will improve detection effectiveness, ultimately improving overall security outcomes. This relationship serves as the study's logical structure, providing consistency between the research questions and the theoretical constructs being studied.

2.4 Review of Related Literature

2.4.1 Historical Background of The Phenomenon

Honey pots were first developed by researchers in the early 1990s. Researchers were looking for ways to monitor hackers within a controlled environment. Clifford Stoll's book "The Cuckoo's Egg," published in 1989, is where researchers first began using decoy systems to learn how attackers behaved. As research continued, honeypots transitioned from an academic tool to a tool used in large-scale cybersecurity environments within enterprises and the cloud.

During the 2000's researchers created low-interaction honeypots such as Honeyd. These honey pots enabled researchers to simulate networks at large scales. Today, researchers have created high-interaction honeypots that can emulate full operating systems. In addition, hybrid honey pots are now available. Hybrid honey pots combine low- and high-interaction honey pots to efficiently gather information about potential threats to your network. The development of honeypots has changed the way researchers and organizations gather threat data. Instead of passively monitoring the actions of potential hackers, honeypots are now being used to actively defend against potential attacks and provide valuable threat intelligence to organizations.

2.4.2 Key Honeypot Concepts in Network Security

Honey pots are systems designed to entice attackers to exploit them based on their vulnerabilities, with the intent of gathering information from the hacker about the types of attacks, the methods used to breach security, and the malware involved in the attack (Spitzner, 2003). Modern honeypots, however, are being utilized as part of the development of threat intelligence – information that would be relevant to a potential adversary's tactics, techniques, and procedures (TTPs) that they may employ against an organization.

Modern Network Security Architecture is a comprehensive architecture that defines how the physical and logical layers of a network should be protected. The architecture includes the policies, hardware, and software that protect organizational systems (Whitman & Mattord, 2022). In terms of Network Security Architecture, Honey Pots can be considered an Active Defense component that provides insight into the actions of attackers attempting to intrude into an organization's systems.

The effectiveness of honey pots is measured using several factors: Detection Accuracy, Data Quality, Scalability, and Integration Capability. A study conducted by Almeshekah and Spafford (2016) reported that the use of honey pots increased the detection accuracy of attackers and the quality of data available for profiling attackers when a honey pot was integrated with a Security Information and Event Management (SIEM) System.

2.4.3 Empirical Studies Related to the Research Variables

Numerous empirical studies support the feasibility of deploying honeypots for operational purposes. According to Naeem (2021), many high-interaction honeypots can uncover attacks that traditional intrusion detection systems have missed, thereby providing additional investigative capabilities. Additionally, an experimental study by Zimba and Chishimba (2020) found that hybrid honeypot configurations can achieve higher accuracy in detecting malicious activity while reducing the number of false-positive alarms in enterprise networks.

According to Mokube and Adams (2022), several real-world problems arise when deploying honeypots in a production environment, including resource utilization and maintenance complexity. Similarly, Hodo et al. (2017) found several legal and ethical considerations in using honeypots, including data privacy concerns when collecting information about attackers' behavior. As a result of these limitations, empirical research continues to demonstrate that honeypots enhance preparedness and enable organizations to develop adaptive response methods.

2.4.4 Summary of Previous Research Findings

Research indicates that Honeypot systems are capable of providing a clear understanding to the behavior of attacks and can also enhance network defenses if well-planned and executed; however, there is disagreement among researchers on how to measure the effectiveness of Honey Pot systems, and how to scale their use in large networks, or integrate them with new technology, i.e., AI and Cloud Security. Although many researchers agree on the benefits of Honeypot systems for research and detection, relatively little research has been conducted on their long-term effects.

2.5 Role of Honeypots in Modern Network Security Architecture

The data from all of these studies consistently support the view that honey pots are both research tools and defensive measures used to protect against cyber threats today. Honey pots provide researchers and defenders with information about potential cyber threats by providing early warning systems to alert them when a malicious user has entered their system and allow them to respond quickly; they also lower the mean time to detect (MTTD) cyber threats (Almeshekah & Spafford, 2016).

The success of honey pot deployments is contingent upon the design of the deployment architectures and how the honey pot is maintained. Additionally, combining honey pots with machine learning-based analytical tools may be able to increase the ability to predict cyber threats earlier. The synthesis of this study states that the purpose of synthesizing literature is to create an interpretive theoretical framework that connects many different types of empirical evidence to guide future research.

2.6 Research Gap

Although Honeypots have been gaining increased recognition from both academia and industry, there remain significant research gaps. One significant gap is the lack of consistent, comparable methods or metrics to measure how well honeypots perform relative to one another across different network types. Additionally, virtually all previous studies on honeypots have relied on qualitative data. Therefore, this leaves a significant gap in terms of developing measurable (quantitative) data regarding the success of honeypots in achieving measurable goals such as detection rates and data value. Lastly, there has been very little research on integrating honeypots into cloud-based, artificial intelligence (AI)-driven security systems, where dynamic scaling is a necessity.

It is crucial to address each of these areas to help move forward with further honeypot research and to validate the use of honeypots in current security environments. This study addresses both the methodologies for implementing honeypots and the results regarding the effectiveness of those honeypots in today's network settings.

2.7 Summary of The Chapter

The literature review in this chapter provided an overview of the application of honeypots within current and future network security architectures, including theories, conceptual frameworks, and empirical research on the implementation and effectiveness of honeypots as part of a proactive defensive and threat intelligence strategy. As such, there are challenges to the development and deployment of honeypots related to performance measurement and reporting, scalability, and integration with newer technologies.

As a result of identifying the limitations of the literature reviewed, this chapter serves as the foundational framework for Chapter Three (Methodology), which will outline the research design, data collection methods, and analysis techniques for the study. Therefore, the synthesis of the insights from the literature reviewed provides the theoretical basis for the design of the methodology and aligns it with the principles of evidence-based research design as outlined by Ormrod (2023).

RESEARCH METHODS

3.1 INTRODUCTION

The methodology for investigating honeypot deployment and impact on modern networks is outlined in this section. The study provides an overview of the methods used to conduct the research, including the study design, population, sample selection process, data collection tools, data analysis techniques, and ethical considerations. Careful consideration has been given to selecting the appropriate methodologies to meet the study's objective of determining how honeypots are employed, identifying the role they play in network operation, and analyzing the value they provide in detecting and preventing cyber threats.

3.2 RESEARCH DESIGN

A Qualitative Case Study Approach was selected as the best method for this research. The approach uses Technical Document Analysis and Expert Interviews to gather information. Using a qualitative approach is the best method for studying Honeypots, as they are complex tools that must be understood in the context of their use within an organization. The Case-Study Design will allow the researcher to explore in great detail how Honeypots have been used across various organizations. The Case-Study Design will also enable the researcher to compare what was expected to occur when using Honeypots with what happened.

A Case-Study Design was the best selection for this research because it will provide:

- Insight into how Honeypots were deployed in the organizations studied and how effective they were in identifying attackers.
- Allow for the analysis of Attacker Behavior based on Honeypot Logs.
- Enable the researcher to identify areas where the expected outcome of deploying Honeypots differed from the actual outcome.

3.3 POPULATION AND SAMPLING PROCEDURES

3.3.1 TARGET GROUPS

The target group comprises:

- Security experts engaged to deploy a security solution.
- Network managers use Intrusion Detection Systems (IDS).
- Companies are deploying Honeypot systems.
- Technical Documentation, logs, and technical configuration data for Honeypot deployment.

Selection Criteria:

- At least some level of knowledge or practical experience in Cybersecurity or Network Defense.
- Use of honeypots/deception technology by an organization.
- Available Technical Documentation/Public Case Study.

Exclusion Criteria:

- Organizations that do not use Honeypots.
- Non-technical personnel/without responsibility for network security.
- Sources of Data Lacking Credibility/Verification.

3.3.2 SAMPLE SIZE AND SAMPLING TECHNIQUE

This research uses purposive sampling (i.e., selecting participants and documents directly related to the assessment of honeypots) to identify those most knowledgeable about deploying honeypots to assess malicious activity. Due to honeypot deployment being highly technical and requiring significant experience/knowledge, this sampling technique will allow researchers to select individuals with high levels of expertise in the area of honeypot deployment.

Number of Participants/Case Studies/Digital Data Included: 3-5 Interviews with Cybersecurity Professionals, 2-3 Honeypot Case Study Organizations. Technical documentation such as logs, deployment guide(s), and Security Reports

The small number of cases studied may limit generalizability, but it is acceptable given the nature of a qualitative case study and the very complex technical information from honeypots that are being analyzed. Participants were selected through purposeful sampling because they had either deployed a honeypot or have experience as a network security professional; this should maximize the potential for useful, relevant and applicable information based on the research questions asked.

3.4 RESEARCH INSTRUMENTS / DATA COLLECTION TOOLS

In addition to using a semi-structured interview guide for data collection, we will also use two other instruments.

1. Semi-structured Interview Guide (instrument)

The semi-structured interview guide was developed to collect expert opinions related to:

- Deploying honeypots
- Challenges encountered during honeypot operationalization
- Evaluating the effectiveness of honeypots in real-world environments
- Integrating honeypots into intrusion detection systems

A semi-structured interview guide allows the researcher to find a balance between consistency and flexibility, providing an opportunity for the researcher to delve into the participants' responses in much more detail as well as to follow up on emerging issues that are not fully covered by the structure of the interview questions themselves.

2. Technical Documents Review

This encompasses:

- Configuration files of the system
- Logs from Honeypots
- Architecture diagrams of deployment
- Reports from Incident Response
- White Papers in the Deception Technology Industry

Examining these Technical Documents aids in a review of operational Information that is relevant to operations and allows for cross-validation of honeypot Functionality among the various Environments studied.

3. Observations Checklist

If evaluating honeypot dashboards or monitoring tools. Focus areas are Alerts created, Types of attacks captured, Response Mechanisms, Reliability & Validity

To maintain rigor:

- Pilot testing was conducted with a single cybersecurity student to validate that the interview questions were clear and understandable.
- The authenticity of technical documentation was verified through cross verification.
- A method of triangulation was used to compare responses from interviews, logs, and documented case studies.

3.5 DATA COLLECTION PROCEDURES

Following ethical practices to ensure privacy and integrity of the research, the researcher conducted a series of steps in collecting the data for this study:

1. Gained consent from each participant and organization when necessary.
2. Located relevant honeypot systems as well as technical documentation about them.
3. Conducted semi-structured interviews with participants (either in person or online) and collected honeypot log files, honeypot configuration files, honeypot operational reports, as well as monitored honeypot system behavior via a dashboard when possible.
4. To maintain consistency across all data collection processes, the same interview guide and checklist were used for each case.
5. The researcher ensured that they complied with ethical standards throughout the entire research process.

3.6 DATA ANALYSIS METHODS

Thematic analysis was conducted on interview data and organizational case studies using manual coding methods to identify commonalities or patterns for example:

- Effectiveness of honeypots to detect threats, Deployment strategies, Behaviors of attackers
- Challenges in operational use of honeypots
- These themes were developed using an inductive method to reduce the chance of a researcher's bias.

Technical Content Analysis

Data sources included system logs, configuration files and deployment diagrams that would provide information about:

- Number of attacks, Kinds of threats detected by honeypot
- Level of interaction with the honeypot (low vs. high-interaction honeypots)
- Information related to indicators of compromise associated with a honeypot attack. Whether a honeypot is integrated with a Security Information Event Management (SIEM), firewalls, etc.

3.7 ETHICAL CONSIDERATIONS

Ethics were maintained throughout the study as follows:

- All participants gave informed consent before participating.
- Confidentiality maintained by keeping organizations and information anonymous.
- Participants were clearly made aware that their involvement in this study was completely voluntary and could withdraw at any time.
- Protections against unauthorized access to participants' data were implemented, such as encryption of data collected and stored.

3.8 VALIDITY, RELIABILITY & TRUSTWORTHINESS

Credibility

A combination of multiple sources (interviews, logs, and documents) for triangulation of views. Participant verification (member checking) to verify the researcher's interpretation.

Dependability

Documentation of each step of collecting data. Consistent application of research tools/instruments.

Confirmability

Objective interpretation of data supported by evidence. Researcher bias was reduced through reflection on the researcher's notes.

Transferability

Contextual details about settings provided allow other researchers to apply findings to similar contexts.

3.9 Summary of Chapter

The above section provides a description of how a qualitative case study design incorporating expert interviews and a review of relevant documents is applied to evaluate the implementation and success of honey pots within current network security architectures. Documented procedures of sampling, collecting data, analyzing data, and maintaining ethics form the basis for providing objective data in Chapter Four.

ANALYSIS AND INTERPRETATION

4.1 Introduction

In this Chapter, the results of the data collection process (study "Implementation and Effectiveness of Honeypots in Modern Network Security") will be analyzed and interpreted to answer the Research Questions (RQs) and Objectives (Os). The RQs and Os were designed to determine how honeypots are implemented and how they detect and prevent attacks as part of a larger effort to analyze and strengthen modern network security architectures.

The data utilized in the study included qualitative interviews with cybersecurity professionals, review of the log files of honeypot activity, and review of published case studies of honeypot use. This Chapter provides an interpretation of the collected data relative to answering the RQs and O.

4.2 Response Rate and Data Screening

In accordance with the methodology identified in Chapter Three, this study used two documented honeypot case studies from organizations and three semi-structured interviews with cyber security professionals in conjunction with supporting technical documentation (i.e., system logs, configuration files, incident reports).

All three interview participants completed their respective interview processes, which resulted in a 100% response rate. A 100% response rate is an acceptable response rate for qualitative case study research, where depth and expertise of respondents is prioritized above sample size.

Both organizational case studies included logs from the actual honeypot deployments and related technical documentation. In addition, all collected data were reviewed to ensure complete and relevant data collection. There were no interview responses or documentation omitted from analysis; all of the sources fit within the inclusion criteria established in Chapter Three.

Documentation was also reviewed to verify that the honeypots being studied represented actual operation systems that were deployed into either real or simulated organizational environments, as opposed to partial or theoretical implementations. The professional backgrounds of all interview participants were also confirmed to have practical knowledge with regard to both intrusion detection systems and honeypot technologies.

4.3 Profile of Study Participants

The three participants in this study included Cybersecurity Professionals with varied functions and levels of experience within the Cybersecurity field. The first participant functioned as a Network Security Analyst, while the second participant worked as an SOC Analyst and the third participant functioned as a Security Researcher that has used Deception Technologies for many years.

All participants have a minimum of two years of professional experience in Cybersecurity and a hands-on knowledge of Intrusion Detection Systems, Honeypots or other types of Defensive Technologies. Based on their experience, they were able to provide knowledgeable insights regarding how to deploy, how effective, and what are some of the common operational challenges associated with Honeypots.

4.4 Presentation of Results According to Research Questions

In order to add more clarity and to add more analytical rigor to the qualitative results, a table is developed to summarize the key trends from the data analysis of the qualitative results. The tables will be used to group themes and should not be a replacement for the narrative interpretation of the qualitative results.

Research Question 1:

What are some typical deployment locations for honeypots in current network security architecture?

Three typical deployment models were identified through an analysis of interviews and documentation of case studies.

The most common deployment model for honeypots was in either the DMZ, or close to a Perimeter Firewall where external recon and brute force attacks could be detected. One case study demonstrated how internal honeypots were used to identify lateral movement inside a network.

Both case studies made extensive use of virtual honeypots due to the lower cost of deploying them compared to physical honeypots. Case studies referenced the use of tools such as Cowrie, Dionaea, and Honeyd. Logs of honeypots showed repeated unauthorized attempts at accessing exposed services on honeypots.

Case Studies also identified honeypot logs being integrated into Security Information and Event Management (SIEM) systems, along with other security systems such as Firewalls and Intrusion Detection Systems (IDS), allowing for centralizing logging and correlating system events across multiple security systems.

Deployment Aspect	**Observed Implementation**	**Evidence Source**
DMZ Deployment	Detections by a Demilitarized Zone Honeypot for Port Scans, Brute-Force Attempts and External Threats.	Interview data, Case Study 1
Internal Network Deployment	Detection of Lateral Movement and Insider Threats through Internal Honeypots.	Interview data
Virtualized Honeypots	Virtual Honeypots (Cowrie, Dionaea, Honeyd) are being utilized for easier and less expensive deployments.	Case Study 1 & 2
Integration with SIEM	Logs from Honeypots are being fed into SIEM Tools for Centralized Monitoring and Alert Correlation.	Case Study 2
Integration with IDS/Firewall	Alerts from Honeypots are being correlated against Logs from Firewalls and IDS systems for better detection.	Interview data

Research Question 2:

What is the effectiveness of using Honeypots to identify Malicious Activity?

The logs from the honeypots examined within this study provided a large amount of indicators of attacks, such as SSH brute force attempts, port scan activity, credential guessing and attempted downloads of malware. The honeypots identified suspicious activity prior to the triggering of an alert by the IDS systems in both cases studied.

It was found that the honeypots nearly eliminated false positives because any interaction between a user and a honeypot would be considered suspicious due to there being no legitimate reasons for a user to interact with a honeypot. It was reported through interviews that all users had legitimate reasons to use the systems they accessed, therefore alerts produced by honeypots were extremely reliable.

In addition, honeypots allowed researchers to identify attack patterns; specifically, the honeypots revealed that hackers were targeting specific commonly open ports (22, 23 and 445) repeatedly, the hackers were using the same sets of credentials and hacking originated from the same locations repeatedly. The knowledge gained from these patterns were then used to enhance firewall rules and access controls.

Attack Type	Targeted Service/Port	Observed Behavior	Security Insight Gained
Brute-force login attempts	SSH (Port 22)	Repeated credential guessing attempts	Strengthened authentication and access controls
Unauthorized access attempts	Telnet (Port 23)	Legacy protocol exploitation attempts	Recommendation to disable insecure services

File-sharing exploitation	SMB (Port 445)	Scanning and exploitation attempts	Improved firewall filtering rules
Port scanning	Multiple ports	Reconnaissance behavior prior to attacks	Early threat detection
Malware download attempts	Various	Attempts to retrieve malicious payloads	Identification of malicious IPs and hashes

Research Question 3:

What issues exist in implementing honeypots?

There have been many advantages of using honeypots; however, there are also several disadvantages to this method. Continuous maintenance of honeypots is needed along with frequent updating of honeypots to avoid fingerprinting by the attacker. One member stated that honeypots will eventually lose their ability to detect an attacker if they are not regularly updated.

Another disadvantage to high interaction honeypots would be if they are not properly segmented from other networks or systems; the attacker may then use the honeypot system to continue launching additional attacks.

Lastly, limited technical skills were seen as a limitation for some organizations. The organization's security team would need to have technical skills to interpret the honeypot logs and integrate them into the existing security workflow.

Challenge Identified	**Description**	**Impact**
Maintenance Requirements	Frequent updates needed to avoid detection by attackers	Reduced effectiveness if neglected

Risk of Misuse	High-interaction honeypots can be exploited if not isolated	Potential security exposure
Skill Requirements	Specialized expertise needed to manage and analyze honeypot data	Adoption barriers for small organizations

4.5 Interpretation of Findings

The research indicates that honeypots are an important component of modern network security and are very useful in detecting emerging attacks and gathering high-quality intelligence for use by organizations; this is consistent with the theoretical foundations presented in the Literature Review section. This research supports prior studies, which include:

- Spitzner (2002), stated that honeypots were capable of discovering unknown threats
- Sokol & Husak (2021), who indicated that honeypots had low false positive rates
- Provos & Holz (2008) who illustrated the effectiveness of virtual honeypots

This research was consistent with prior studies and demonstrated that honeypots continue to be effective in modern network architectures.

4.6 Discussion of Key Findings

Significant results have been generated:

1. Early threat detection by Honeypot systems compared to traditional security systems.
2. This implies that a supplementary threat detection layer is added to enhance overall network protection.
3. Low noise quality data is produced by Honeypot systems.
4. Reduced SOC workloads and increased accuracy in incident investigations as a result.

5. Virtual Honeypots are preferred due to their affordability, scalability, and ease of deployment. However, several challenges exist, including monitoring, containment, and required expertise.

The results demonstrate that, although Honeypots are not a replacement for Firewalls or IDS, when properly integrated, they will greatly increase security.

4.7 Summary of the Chapter

In this chapter, we present and analyze data gathered from interviews, documentation review, and honeypot activity log files. We will discuss our results by addressing each of the study's research questions: Implementation, Effectiveness, and Challenges.

Our results show that Honeypots are an effective way to detect malicious behaviors, can produce very useful information for threat intelligence, and can significantly contribute to a better security architecture. However, the honeypots must be properly monitored, isolated, and managed with experienced personnel. I will summarize my findings, conclude, and offer recommendations for future research.

Summary, Conclusions, and Recommendations

5.1 Overview

This section of the report presents the study's conclusion (Implementation and Effectiveness of Honeypots in Modern Network Security Architecture) and outlines the main points discussed throughout the study. This will include an overview of the entire study, the most important information gathered from the data collection phase (the analysis phase), and, finally, practical recommendations for organizations interested in implementing honeypots within their network security strategy.

5.2 Summary of Study

Traditional security measures alone are no longer sufficient due to the rise in cyberattacks and increasingly sophisticated threats to networks. Organisations are finding it increasingly difficult to detect unknown threats, insider threats, and Advanced Persistent Threats (APTs) using Firewalls, Intrusion Detection Systems (IDSs), Anti-Virus software, etc. This research addresses the question of whether and how honeypots could improve modern network security architectures by enhancing threat detection and attacker analysis capabilities.

The primary objective of this study was to investigate the implementation and effectiveness of honeypots in modern network security architectures. More specifically, the objectives were to determine whether honeypots can identify malicious activity, analyse the behaviour of attackers, and integrate with other current security technologies, including SIEM systems.

A structured research methodology was used for this study. The populations studied for this research were network security environments that deploy honeypots for monitoring and analysis purposes. Based on simulated network traffic and security events generated from honeypot systems, a representative sample was selected. The data collected through deployment of honeypots under controlled conditions, log analysis, and the observation of attack patterns.

Key findings from the study were:

Honeypots are effective at capturing unauthorized access attempts, especially when targeting services such as SSH, Telnet, and SMB. Honeypots offer significant insight into the techniques attackers use and can assist organisations in developing an appropriate and timely response to incidents. In summary, the study concluded that honeypots can be a valuable asset to modern network security architectures.

5.3 Summary of Key Findings

In addition to the study’s objectives and research questions, the summary below is based on the study's findings:

Firstly, the study demonstrated that honeypots have proven successful in identifying potential malicious activities that would otherwise go undetected by standard security technologies. In addition, the honeypots allowed the researchers to document hackers' activity without affecting operational systems; therefore, providing additional information on how hackers operate.

Secondly, the study found that hackers most commonly targeted standard services such as SSH, Telnet, and SMB; thus, demonstrating the need for continuous monitoring of these services and stronger configuration of security controls in the real-world environment.

Thirdly, the study demonstrated that honeypot-generated data can be successfully utilized in conjunction with SIEM systems. The use of both honeypot and SIEM data will enhance centralized monitoring, improve alerting, and enable better correlation of security-related events.

Lastly, the study found that honeypots will enable security personnel to gain a clearer understanding of hackers' actions, enabling them to develop better procedures for responding to incidents and to better plan for future security-related issues.

5.4 Conclusions

Based on the study findings, it was determined that honeypots are a viable method for security professionals to detect and analyze malicious activities in today's complex networked environment. Additionally, the study provided support for established cybersecurity theories, including defense-in-depth and proactive threat detection through the use of honeypots as an additional layer of intelligence gathering that complements other control methods used in preventative and detective controls.

5.5 Recommendations

As a result of this study's conclusions, the following recommendations are made:

Policy Recommendations, Organizations and Institutions should consider incorporating Honeypot deployment within their Cybersecurity Policies. Guidelines for monitoring, Data Handling, and Ethical Use of Honeypots should be created and implemented.

Practical Recommendations, Security Teams should implement Honeypots to integrate the collected logs from the Honeypot(s) with their SIEM platform, enabling centralized log analysis and real-time alerting. Honeypots should be strategically located to monitor High-Risk Services such as SSH and SMB.

Academic and Research Recommendations, Educational Institutions should incorporate Hands-On Honeypot Labs within their Cybersecurity Curricula to provide students with enhanced Practical Learning Opportunities. Researchers should continue researching Advanced Honeypot Technologies and their role in detecting Emerging Threats.

5.6 Contribution to Knowledge

This study has contributed to the Cybersecurity Body of Knowledge by providing insight into the effective implementation of Honeypots in Modern Network Security Architecture and demonstrating how Honeypots can be used as a Proactive Threat Detection Tool, in conjunction with traditional security mechanisms.

This study has also contributed to the body of knowledge by validating the integration of Honeypots with SIEM Systems and demonstrating how these two tools can work together to improve Threat Intelligence and Incident Response Capabilities.

These contributions to the body of knowledge have added to existing knowledge regarding the practical uses of Honeypots in Real-World Security Environments.

5.7 Suggestions for Future Research

Although this study has provided many useful insights into the use of Honeypots, several areas warrant additional research. Additional research can be conducted to determine whether Low-Interaction or High-Interaction Honeypots are more effective in specific Network Environments. Research can also be conducted using Machine Learning Techniques to analyze data collected by Honeypots and Improve Automated Threat Detection.

Expanding upon this study to utilize Larger Datasets and Real-World Organizational Deployments will add greater credibility and validity to the results obtained through this research.

5.8 Summary of the Chapter

This Chapter provides a summary of all aspects of the research study (research question, literature review, methodology, results, and discussion), identifies the most important findings of the study, and draws conclusions regarding the Effectiveness of Honeypots in Modern Network Security Architecture. This Chapter has also provided the reader with practical suggestions for using Honeypots in the workplace, discussed how this study contributes to our overall knowledge base in Cybersecurity, and identified several areas for future research.

References

Naeem, A. A. N. (2021). Honeypots: Concepts, approaches and challenges [Preprint]. HAL Open Science. https://hal.science/hal-03324407/document

Javadpour, Amir, et al. "A Comprehensive Survey on Cyber Deception Techniques to Improve Honeypot Performance." Computers & Security, vol. 140, 1 Mar. 2024, www.sciencedirect.com/science/article/pii/S0167404824000932, https://doi.org/10.1016/j.cose.2024.103792.

Ormrod, J. E. (2023). Practical research: Design and Process (13th ed.). Pearson Education.

Horcas, Jose-Miguel, et al. "An Approach for Deploying and Monitoring Dynamic Security Policies." Computers & Security, vol. 58, May 2016, pp. 20–38, https://doi.org/10.1016/j.cose.2015.11.007. Accessed 26 Sept. 2020.

Mokube, I., & Adams, M. (2022). Honeypots: Concepts, approaches, and challenges. Journal of Information Security Research, 8(3), 45–56. https://hal.science/hal-03324407/document

Provos, Niels. A Virtual Honeypot Framework. 2003. https://www.cs.unc.edu/~jeffay/courses/nidsS05/honeypots/citi-technical-report.pdf

Omar, Amira Hossam Eldin, et al. "An Innovative Honeypot Architecture for Detecting and Mitigating Hardware Trojans in IoT Devices." IoT, vol. 5, no. 4, 31 Oct. 2024, pp. 730–755, https://doi.org/10.3390/iot5040033.

Yilmaz, Fadi, et al. "A Fine-Grained Classification and Security Analysis of Web-Based Virtual Machine Vulnerabilities." Computers & Security, vol. 105, June 2021, p. 102246, https://doi.org/10.1016/j.cose.2021.102246. Accessed 15 Nov. 2021.

Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic inquiry. SAGE Publications. — Foundation for credibility, dependability, confirmability, and transferability.

"Spitzner, L. (2002) Honeypots Tracking Hackers. Addison-Wesley, Boston. - References - Scientific Research Publishing." Scirp.org, 2022, www.scirp.org/reference/referencespapers?referenceid=3300232.

Stallings, William. Global Edition Network Security Essentials Applications and Standards Sixth Edition.

Franco, Javier, et al. "A Survey of Honeypots and Honeynets for Internet of Things, Industrial Internet of Things, and Cyber-Physical Systems." IEEE Communications Surveys & Tutorials, vol. 23, no. 4, 2021, pp. 1–1, https://doi.org/10.1109/comst.2021.3106669.

Li, Jiachun, and Guoqian Chen. "A Personalized Trajectory Privacy Protection Method." Computers & Security, vol. 108, Sept. 2021, p. 102323, https://doi.org/10.1016/j.cose.2021.102323. Accessed 3 Aug. 2021.

Thonnard, Olivier, and Marc Dacier. "A Framework for Attack Patterns' Discovery in Honeynet Data." Digital Investigation, vol. 5, Sept. 2008, pp. S128–S139, https://doi.org/10.1016/j.diin.2008.05.012. Accessed 11 Jan. 2021.

Virtual Honeypots Know Your Enemy. https://troopers.de/media/filer_public/38/ad/38ada17d-d73f-4821-808b-f2f4a023c0a3/holz_thorsten_-_virtual-honeypots.pdf