Department of IT and Computer Science

Faculty of Electrical, Computer, IT and Design

Pak-Austria Fachhochschule: Institute of Applied Sciences and Technology, Haripur, KPK, Pakistan

Project Proposal
for

Hive Sentinel:
Control Management System of Honeypots.

Version 1.0

By

Mariyam	**B20F0165CS004**
Muhammad Qaseem Ul Hassan	**B20F0279CS013**

Supervisor

Dr. Abdul Waheed Khan

Bachelor of Science in Computer Science (2020-2024)

Table of Contents

1. Project Title

Hive Sentinel: Control Management System of Honeypots

2. Problem Statement

Honey pots refers to decoy systems or resources that are intentionally set up to attract and monitor unauthorized access attempts. They are used as a proactive security measure to detect, analyse, and gather information about attackers and their techniques.

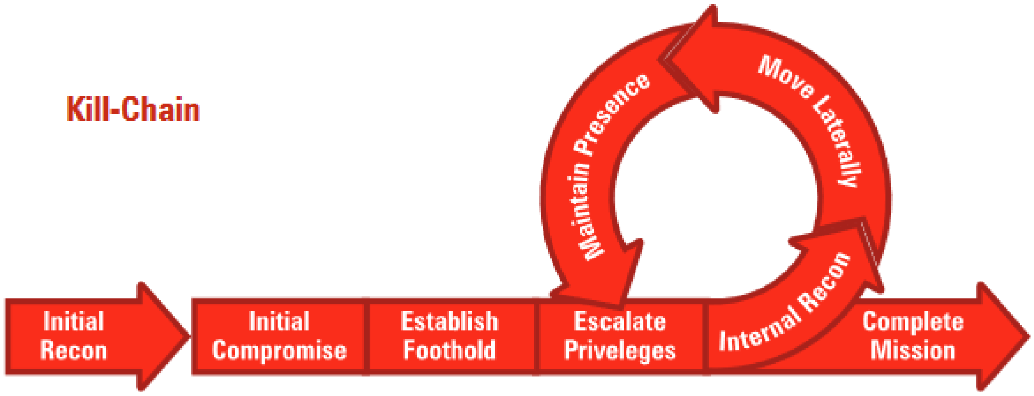
The lack of a dedicated health monitoring system for honeypots can lead to significant consequences for an organization's cybersecurity. Firstly, there is a risk of a false sense of security. If a honey pot is not functioning properly, it may fail to detect and capture malicious activities effectively. This can create a misleading belief that the network is adequately protected, leaving critical assets vulnerable to real threats. Secondly, the organization may face limited or inaccurate threat intelligence.

A compromised or malfunctioning honey pot may provide unreliable or incomplete information about attacker tactics and tools. This hampers the organization's ability to gather accurate threat intelligence, hindering their capacity to make informed decisions and take appropriate security measures. Furthermore, a vulnerable honey pot can introduce additional risk and exposure. Attackers can exploit the compromised honey pot as an entry point to infiltrate the network or gain insights into the organization's infrastructure. This not only undermines the effectiveness of the honey pot but also puts other systems and valuable assets at risk.

3. Framework and Methodology.

3.1 **The Kill-Chain Model**

The "kill-chain" model delineates the stages of an advanced threat attack, from initial compromise attempts thwarted by perimeter security to persistent infiltration via methods like social engineering or phishing. Once inside, the threat escalates privileges, surveys the network, and moves laterally to target the next vulnerable point.



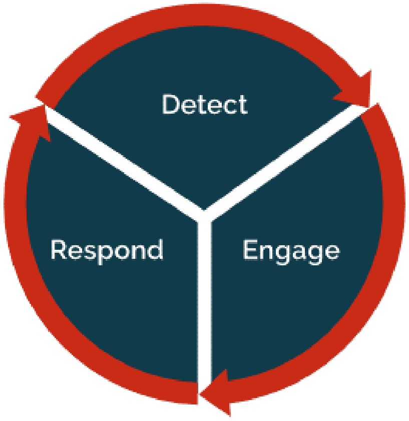
3.2 **DETECT, ENGAGE & RESPOND**

To combat advanced threats, comprehensive mitigation demands a deep understanding of their tactics and procedures. Deception solutions operate in three key phases: **Detect, Engage, and Respond**, interacting with threats at various levels. This systematic approach ensures effective detection and mitigation strategies, essential in the face of sophisticated exploits.

Detect: Unveiling Threats Confidently
During this phase, any interaction with deception methods uncovers potential threats, be it through fake privileges or network shares. However, while crucial, mere detection is not adequate for comprehensive threat elimination.

Engage: Detailed Intelligence Gathering
Once detected, engagement begins using high-interaction deception techniques such as servers and routers. These methods mirror production resources and enable the collection of intricate details about threat tactics, payloads, command centers, and compromised accounts.

Respond: Strategic Mitigation and Automated Remediation
Understanding the attacker's techniques informs the formulation of strategic responses. Automated intelligence correlates the acquired threat intelligence, facilitating the development of response strategies. These responses, including actions like shutting down access to external exfiltration sites, effectively slow down attacks and remediate vulnerabilities.



3.3 **Pervasive Deception: Comprehensive Strategy.**

Deception tactics come in various forms, strategically placed throughout the entire attack process. These tactics can be categorized into two main types:

- **Decoys**: Tempting Targets

Decoys are artificial systems or software services designed to lure attackers. Honeypots exemplify this concept, alongside decoys like routers, printers, or databases. These decoys often hold enticing data and well-known vulnerabilities, making them more attractive to attackers than real production network assets.

- **Breadcrumbs**: Guiding the Attack

Breadcrumbs are crucial in guiding attacks toward decoys. Given that initial compromises typically occur on enterprise endpoints, strategically placed breadcrumbs on endpoints and within networks direct attackers toward these decoy targets.

Pervasive deception is required at every stage of the kill chain to disrupt the attacker.

3.4 **Conditions for Effective Threat Engagement in High-Interaction Honeypots**

- **Comprehensive Deception Setup:**

The honeypot must feature multiple decoys, breadcrumbs, and baits strategically installed to identify exploits used and lateral movement paths.

- **Interconnected Decoys for Lateral Movement:**

Lateral movement within the network should lead the attacker to other decoys, enhancing the honeypot's effectiveness.

- **Invisible Collection Mechanism:**

The collection mechanism must remain invisible to the attacker, ensuring covert monitoring of their activities.

- **Network Traffic Analysis:**

Capture and correlation of network traffic with the attacker’s actions, aiding in identifying command and control centers, exfiltration activities, etc.

- **Comprehensive Attacker Action Logging:**

Record all attacker actions using methods like instrumented binaries, screen capture, and keyboard loggers to gain detailed insights.

- **Memory Dump Analysis:**

Capability to review memory dumps to identify any files not saved to disk, providing a deeper understanding of the attacker's activities.

- **Tracking Downloaded or Dropped Files:**

Ability to track downloaded or dropped files, enabling the analysis of potentially malicious content.

3.5 **Implementing Deception 2.0**: Enhancements and Innovations

1. **Hybrid Interactivity**: Deception 2.0, known as Fluid Deception, seamlessly merges low and high-interaction approaches, offering a versatile range of interactivity options.

2. **Simplicity in Low-Interaction Deceptions**: Customized low-interaction services in Deception 2.0 steer clear of emulations, ensuring comprehensive coverage and resistance against fingerprinting techniques.

3. **Scalability**: Fluid Deception efficiently tackles deployment scale challenges, adapting seamlessly to diverse operational needs.

4. **Mitigating Fingerprinting Risks**: Employing a dynamic approach, Deception 2.0's DevOps model deploys real services instead of emulations, reducing the risk of fingerprinting. It also ensures ongoing freshness to avoid staleness.

5. **Ease of Management**: Deception 2.0's automated DevOps model simplifies deployment and maintenance, enhancing user experience and operational efficiency.

6. **Enhanced Security Measures**: Deception farms and projection points are employed, significantly reducing the risk of compromise and enhancing overall security posture.

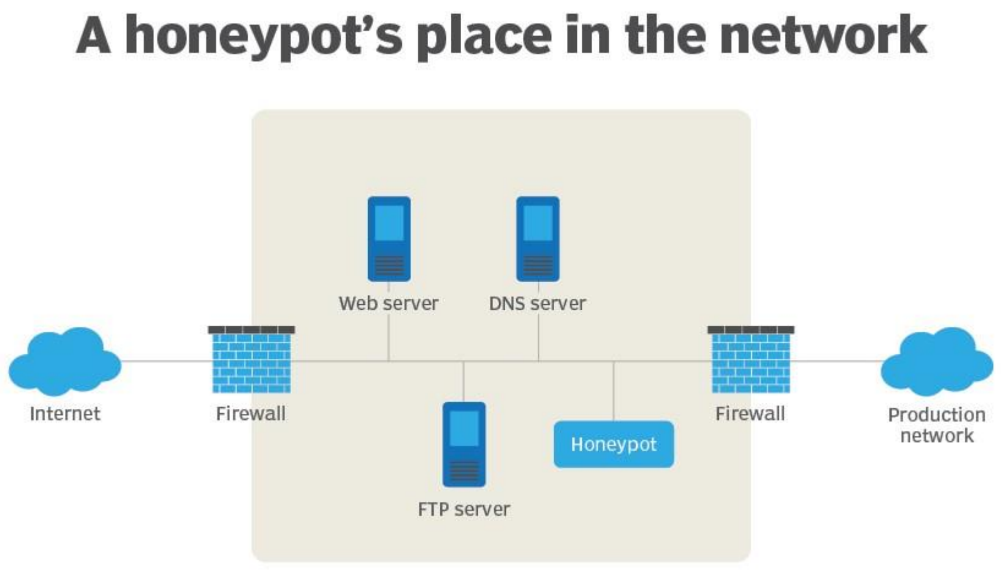
7. **Expanded Scope of Deceptions**: Unlike its predecessor, Deception 2.0 goes beyond traditional honeypots, mimicking a wide array of enterprise resources for a more comprehensive approach.

8. **Integration with Security Ecosystem**: Deception 2.0 actively interacts with the broader security ecosystem, providing valuable input and intelligence, making it a dynamic component of overall threat mitigation strategies.

9. **Integrated Threat Analysis**: Threat engagement and analysis are intrinsic components of Deception 2.0, ensuring continuous vigilance and proactive responses to emerging threats.

4. Objectives:

1. Design and implement a comprehensive control management system specifically tailored for honeypots.
2. Continuously monitor the health, performance, and security of honeypots, including system resources, network connectivity, and application services.
3. Detect and alert administrators about suspicious or malicious activities targeting the honeypots in real-time.
4. Incorporate security measures, such as encryption, access controls, and intrusion detection, to safeguard collected data.
5. Provide detailed logs, reports, and analysis of honeypot activities for threat intelligence purposes.
6. Implement snapshot restoration capabilities to reset honeypots to a clean state after attacks or specific penetration levels.
7. Integrate the monitoring system with other security infrastructure, such as SIEM systems, for centralized monitoring and correlation of security events.



5. Challenges:

1. Identifying and monitoring a wide range of honeypot types, including network-based, service-based, and client-based honeypots.
2. Ensuring real-time monitoring and detection of attacks while minimizing false positives.
3. Integrating with different honeypot frameworks and technologies, considering their diverse architectures and configurations.
4. Handling large volumes of logs and data generated by multiple honeypots for analysis and storage.
5. Safeguarding collected data with security measures to prevent unauthorized access and maintain privacy.
6. Designing efficient and scalable monitoring mechanisms to accommodate a potentially large number of honeypots.
7. Providing actionable insights and reports for administrators to make informed decisions.

8. Scope of the project

5.1 **Honeypot Control Management and Health Monitoring**

- Develop a comprehensive control management system tailored for honeypots.
- Monitor system resources, network connectivity, and application services
- Implement security measures such as encryption, access controls, and intrusion detection systems.

5.2 **Log Analysis and Threat Detection**

- Analyse logs generated by honeypots, including Sysmon and Auditd
- Detect and alert control manager about suspicious or malicious activities in real-time.
- Map detected activities to the MITRE Attack/Defend framework for better understanding and response

5.3 **Snapshot Restoration and Resilience**

- Implement snapshot restoration capabilities to reset honeypots to a clean state after attacks or specific penetration levels
- Ensure honeypots remain effective while maintaining overall security

5.4 **Threat Reporting**

- Generate detailed logs, reports, and analysis of honeypot activities

- Contribute to the organization's threat intelligence program

5.5 **Integration with Security Infrastructure**

- Integrate the monitoring system with other security infrastructure, such as SIEM systems - Enable centralized monitoring and correlation of security events

The project creates a comprehensive honeypot monitoring system for health monitoring, log analysis, threat detection, and snapshot restoration. It enhances incident response, strengthens network protection, and aligns with the MITRE Attack/Defend framework.

9. Functionalities

1. Continuous monitoring of system resources, network connectivity, and application services of honeypots.

2. Real-time detection and alerting of suspicious or malicious activities targeting the honeypots.

3. Implementation of security measures, including encryption, access controls, and intrusion detection systems.

4. Snapshot restoration capabilities to reset honeypots to a clean state after attacks or specific penetration levels.

5. Generation of detailed logs, reports, and analysis of honeypot activities for threat intelligence purposes.

6. Integration with other security infrastructure, such as SIEM systems, for centralized monitoring and correlation of security events.

10. Utilitarian/Application aspects

• **Cybersecurity Research:**

- Hive Sentinel aids cybersecurity research by gathering information on emerging threats, attacker techniques, and trends.

- It contributes to the development of proactive defense measures and improves understanding of cyber threats.

• **Incident Response:**

- The monitoring system enables real-time alerts and insights into potential attacks, facilitating prompt and effective incident response.
- Control manager can take immediate action to mitigate threats and minimize the impact on the organization.

• **Threat Intelligence:**

- Hive Sentinel generates detailed logs, reports, and analysis of honeypot activities, providing valuable information for threat intelligence programs.
- It enhances the organization's understanding of threat actors, their tactics, techniques, and procedures (TTPs), and supports proactive defense strategies.

• **Network Protection:**

- By diverting attacks to honeypots, Hive Sentinel safeguards the production systems from being compromised.
- It reduces the risk of data breaches and disruptions, ensuring the integrity and availability of critical network resources.

11. Proposed tools and platforms

• **Virtualization and Orchestration:**

- Utilize KVM and Ansible for efficient provisioning, deployment, and scalability of honeypots.
- Enables flexible management of virtualized honeypot environments, optimizing resources.

• **Process Monitoring:**

- Implement Sysmon and Auditd to gain insights into process activities within the honeypot environment.
- Detect adversary techniques mentioned in the MITRE ATT&CK framework by monitoring process behaviour.

- **Security Infrastructure Integration:**

- Integrate the monitoring system with SIEM systems for centralized monitoring and event correlation.

- Enhances threat intelligence and aligns with MITRE's recommendations for comprehensive security operations.

- **Encryption and Access Controls:**

- Implement robust encryption mechanisms and access controls to safeguard sensitive honeypot data.

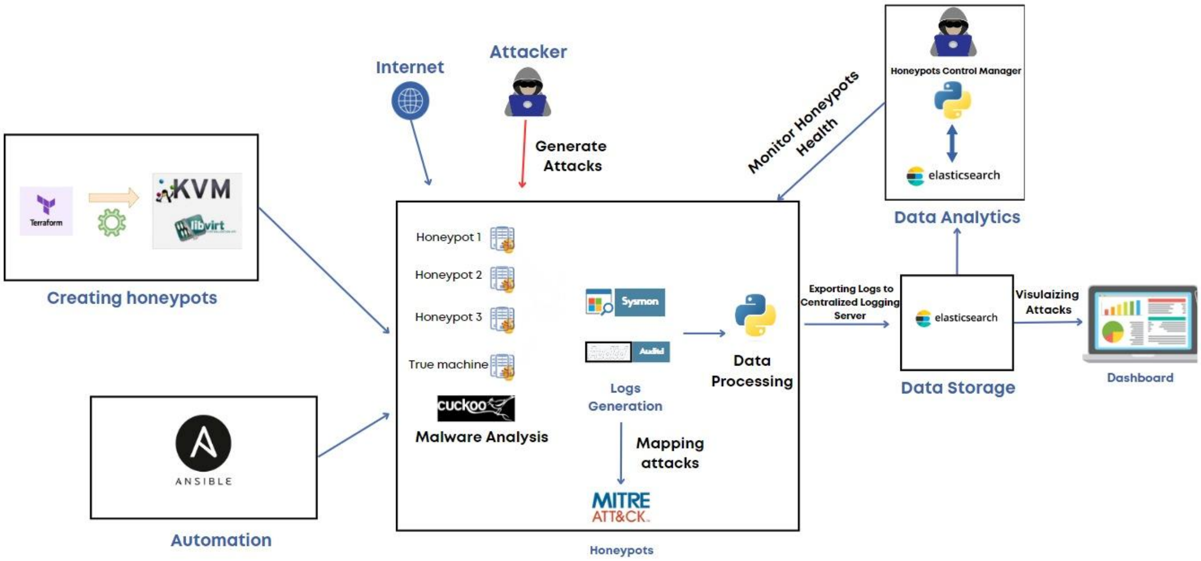
- Protect against unauthorized access, manipulation, or disclosure, ensuring data confidentiality and integrity.

- **Logging and Reporting:**

- Utilize logging frameworks and reporting tools to capture detailed honeypot activity logs.

- Generate comprehensive reports aligned with MITRE's recommendations for threat intelligence and incident response.

12. Architecture Diagram



13. Acknowledgement

We would like to express our gratitude to **Dr. Nabeel Ahmad**, our industrial supervisor at **Cydea Tech**, for their support as we begin the proposal phase of my Final Year Project. We are thankful for their guidance and expertise. We also appreciate the support of **Cydea Tech's management and staff**, as well as our academic advisor, **Dr. Abdul Waheed Khan**.