Internal assessment Report on

HoneyPot using PentBox

by

Parth Pancholi 16010121128
Raheel H Parekh 16010121133
Ujjawal Patel 16010121139

For the subject

Information Security

Department of Computer Engineering
K. J. Somaiya College of Engineering
(Constituent College of Somaiya Vidyavihar University)
Academic Year 2023-24

Under the guidance of:

Prof. Swati Mali

Topic chosen: Honeypot

Introduction

A honeypot is a cybersecurity mechanism designed to attract and detect malicious activity within a network or system. The concept behind a honeypot is to act as a decoy, enticing attackers to interact with it, thereby providing valuable insights into their methods and motives. The primary goal is to enhance the overall security posture by studying and understanding cyber threats in a controlled environment. The digital landscape is fraught with threats, making cybersecurity a paramount concern for organizations worldwide. In response, innovative security measures like honeypots have emerged. This report delves into the concept of honeypots, their functionality, types, deployment strategies, and their role in enhancing cybersecurity.

Types of Honeypots:

- Research Honeypots: Deployed to gather intelligence on threats and attackers.
- Production Honeypots: Integrated into a network's defense strategy to deflect and analyze attacks in real-time.
- Low-Interaction Honeypots: Emulate a limited set of services, suitable for detecting automated attacks.
- High-Interaction Honeypots: Fully simulate real systems, providing comprehensive insights into attacker behavior.

Features/Characteristics:

Deception:

Honeypots rely on deception, appearing as legitimate targets to attract potential attackers.

They can mimic various systems, services, and vulnerabilities to create a realistic environment.
Isolation:

Honeypots are often isolated from the production network to prevent any potential impact on critical systems and data.
Network segmentation ensures that the honeypot operates independently, minimizing risks.
Passive and Active:

Passive honeypots observe and log activities without interacting with attackers.
Active honeypots engage with attackers, collecting more detailed information about their techniques.
Low Interaction and High Interaction:

Low-interaction honeypots simulate only the most basic services, reducing the risk of compromise.
High-interaction honeypots replicate real systems, allowing for a more comprehensive understanding of attacker behavior.
Emulation and Virtualization:

Honeypots can emulate specific operating systems, services, and applications to convincingly mimic real environments.

Virtualization technologies enable the deployment of multiple honeypots on a single physical machine, optimizing resource usage.
Methodology:

Deployment:

Select an appropriate type of honeypot based on the objectives (research, detection, or analysis).
Deploy honeypots strategically within the network, considering the organization's infrastructure and potential attack vectors.

Configuration:

Configure the honeypot to mimic authentic systems, services, and vulnerabilities to attract a diverse range of attackers.
Ensure that logging and monitoring mechanisms are in place to capture detailed information about the interactions.
Monitoring and Analysis:

Actively monitor the honeypot for any suspicious or malicious activities.
Analyze the captured data to understand the tactics, techniques, and procedures employed by attackers.
Incident Response: If malicious activity is detected, use the information gathered to enhance incident response capabilities.
Isolate and analyze malware samples or other artifacts for further investigation.

Insight into Threat Landscape:

Honeypots provide valuable insights into the evolving threat landscape, helping organizations stay ahead of emerging cybersecurity risks.
Identification of Attack Techniques:

Detailed analysis of honeypot interactions reveals the specific techniques and tools used by attackers.
Forensic Data:

Honeypots generate forensic data that can aid in understanding the scope and impact of a security incident.
Enhanced Security Measures:

Organizations can use information from honeypots to improve security measures, patch vulnerabilities, and implement proactive defenses.

Conclusion:

In conclusion, honeypots play a crucial role in cybersecurity by offering a proactive approach to understanding and mitigating cyber threats. Their deceptive nature and ability to attract malicious actors provide a unique vantage point for organizations to strengthen their defenses. However, it's essential to implement honeypots with careful planning, ensuring that they are well-integrated into an organization's overall security strategy. As cyber threats continue to evolve, honeypots remain a valuable tool for staying one step ahead in the ongoing battle against cybercrime.

Github Repository link:

We have stated the commands we have used to implement the tool in the README file of this repository and also attached a copy of this report in the repository.

https://github.com/raheelhp/HoneyPot