جامعة بيرزيت

BIRZEIT UNIVERSITY

Faculty of Engineering and Technology

Computer Science Department

Computer Security (COMP432)

Case Study of Honeypots in Cybersecurity

....

Group Members:

Name	ID
Ibrahim Abu Hijleh	1203065
Osama Manasrah	1203378
Beesan Ajaj	1200943

Under supervision: Dr. Hafez Barghouthi

Date: 11/1/2025

Abstract

In today’s interconnected digital landscape, vulnerabilities in information systems demand innovative security measures. Honeypots, defined as "computer security mechanisms set to detect, deflect, or counteract unauthorized use of information systems," are proactive tools for cybersecurity. Rather than passively awaiting attacks, honeypots actively attract cybercriminals, providing valuable insights into attacker behavior. This paper explores honeypots by addressing key research questions: "What are honeypots?", "Why are they used?", "What are their types and paradigms?", and "How do they achieve their purpose?" The report also provides a technical overview of honeypot operations, discusses their advantages and limitations, and evaluates their evolution.

Table of Contents

History

The History of Honeypots and Deceptions

Honeypots and deception have a rich history, evolving from ancient strategies to sophisticated cybersecurity tools. The following summarizes their development and significance.

Historical Context of Deceptions

Deception has been integral to warfare and strategy for thousands of years, with roots in Sun Tzu's *The Art of War* (800 B.C.) and natural behaviors like baboons' displays of dominance. Cognitive studies by authors such as Chuck Whitlock and Thomas Gilovich have revealed how psychological limits and reasoning fallibility are exploited in deception. These principles extend to military strategies and modern information protection.

Early Computer Deceptions

Computer systems began adopting deception for security, such as login mechanisms that obscure whether a user ID exists. Other long-used techniques include encryption, steganography, and traps, which introduce uncertainty to deter attackers.

Key Milestones in Honeypot History

- **1990/1991**: Early works on honeypots, *The Cuckoo's Egg* by Clifford Stoll and Bill Cheswick's "An Evening With Berferd," lay the foundation.
- **1991**: AT&T researchers develop a real-time "Jail" to track attackers.
- **1997**: Fred Cohen releases the *Deception Toolkit* (DTK), one of the first honeypot solutions.
- **1998**: Development begins on CyberCop Sting, a commercial honeypot.

Advances in Honeypot Technologies

- **Deception Toolkit (DTK)**: Simulates legitimate services using finite state machines to confuse attackers.
- **D-WALL**: Simulates large computer networks via address translation.
- **Invisible Router (IR)**: Introduces protocol-level deceptions like mirroring and dazzlements.

- **Responder**: A versatile tool for custom packet handling and emulation.
- **Execution Wrappers**: Direct unauthorized programs to decoy environments, enhancing insider threat defenses.

The Role of Honeypots Today

Honeypots have advanced from simple tools to sophisticated technologies critical for cybersecurity. Their evolution demonstrates their effectiveness in deterring and studying attackers, while broader deception strategies continue to innovate information protection.

Honeypot Definition and Content

First of all, a honeypot is a computer system. There are files, directories in it just like a real computer.

However, the aim of the computer is to attract hackers to fall into it to watch and follow their behavior.

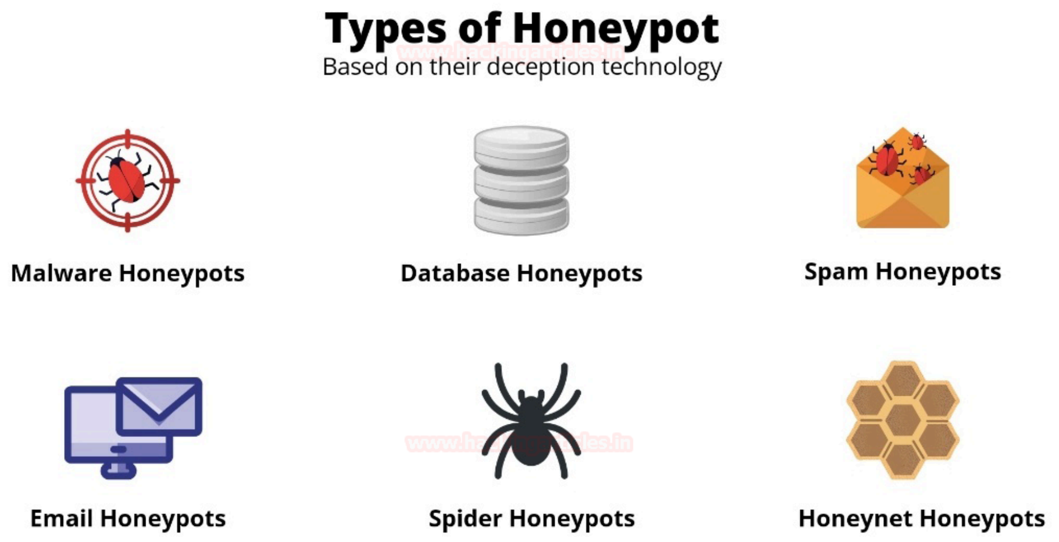
So we can define it as a fake system which looks like a real system.
They are different from other security systems since they are not only finding one solution to a particular problem, but also they are eligible to apply a variety of security problems and finding several approaches for them. For example, they can be used to log malicious activities in a compromised system, they can be also used to learn new threats for users and create ideas how to get rid of those problems.
According to Mokube,I. & Adams M.(2007:p.322) we can divide honeypots according to their aims and level of interactions. If we look at the aims of the honeypots, we can see that there are two types of honeypots, which are research honeypots, and production honeypots.

Types of honeypots: Production vs Research Honeypot

Research honeypots are primarily utilized by military, research, and government organizations to collect vast amounts of information. Their main objective is to discover new threats and gain insights into the motives and techniques of Blackhat hackers. These honeypots aim to enhance system protection by studying adversaries, though they do not provide direct value to the immediate security of an organization.

Production honeypots, on the other hand, are designed to safeguard companies from attacks. These honeypots are deployed within production networks to improve overall security. They typically collect a limited amount of data and often involve low-interaction honeypots. Security administrators monitor hacker activities closely and work to mitigate risks that could affect the organization. However, using production honeypots comes with its own risks. For example, during security testing, unforeseen actions may occur, such as the misuse of other systems through honeypot features. If network administrators are unaware of these potential issues, they could inadvertently expose the organization to significant threats.

Spitzner (2002) suggests that it is helpful to categorize the phases of honeypots into groups. He refers to Bruce Schneier's model as a useful framework for understanding honeypots. Schneier divides security issues into three main steps: prevention, detection, and response.



Advantages of Honeypots

Honeypots are valuable tools that security teams can leverage to enhance network safety. They offer a range of benefits that contribute to a more secure and resilient cybersecurity strategy.

1. Breaking Down the Attacker Kill Chain

Attackers often behave like predators, scanning networks and searching for vulnerabilities. Honeypots serve as decoys that attract attackers, enticing them to engage with fake resources rather than actual sensitive data. This disrupts the kill chain by diverting attackers’ attention and resources toward the honeypot, effectively wasting their time and effort.

2. Testing Incident Response Processes

Honeypots provide an efficient way to evaluate how security teams and systems respond to threats. By simulating real attacks, honeypots help organizations identify weaknesses in their incident response plans and refine their security policies. This proactive testing strengthens overall preparedness against actual threats.

3. Straightforward and Low Maintenance

Honeypots are relatively easy to implement and require minimal ongoing maintenance. Once deployed, they can operate effectively without constant monitoring or extensive customization. Security teams can wait for attackers to interact with the honeypot and gain valuable insights without needing to arm the system with prior threat intelligence.

4. A Rich Source of Information and Real-Time Data Collection

Honeypots act as a powerful tool for collecting real-time data on malicious activities. They can provide detailed insights into attackers' methods, tools, and behaviors, even in cases where encryption is used to hide activities. This information helps organizations better understand evolving threats and improve their defenses accordingly.

Honeypots Detection

Detection is the act of detecting any malicious activity in the system. We are assuming that prevention did not work so one way or another, a hacker compromised the system. There are some ways for detecting those attacks. The well-known detection solution is Network Intrusion Detection Systems. This technology will help users to know if the network is compromised, but it will not prevent hackers from attacking the system. For companies, such detection systems are expensive. At this point, honeypots are valuable to monitor the activity.

Limitations and Challenges:

Honeypots are valuable tools in cybersecurity, but they also come with limitations and challenges. Understanding these issues is crucial to deploying them effectively. Below is a detailed analysis:

1. Limited Scope:

- Narrow Viewpoint:
  Honeypots only collect data on activities directly targeting them. They do not provide insight into attacks on other systems that do not interact with the honeypot.
- Specific Use Cases:
  They are not substitutes for comprehensive security measures like firewalls, intrusion detection systems (IDS), or endpoint protection.

2. Risk of Exploitation:

- Turned Against the Defender:
  If poorly configured, attackers could exploit a honeypot to launch further attacks (e.g., using it as a relay or foothold into other systems).
- Attracting Malicious Traffic:
  A honeypot may unintentionally draw attention from attackers, increasing the risk to nearby legitimate systems.

3. Maintenance Challenges:

- ***Resource Intensive:***
  High-interaction honeypots require significant resources to deploy, monitor, and maintain. They may involve setting up real systems that mimic production environments.

- ***Continuous Updates***:
  To remain effective, honeypots must be regularly updated to reflect current technologies and vulnerabilities.

4. Legal and Ethical Concerns:

- ***Privacy Violations:***
  Monitoring attackers could inadvertently involve collecting sensitive information, raising ethical and legal questions.

- ***Liability Issues:***
  If an attacker uses a honeypot to harm other systems, the honeypot operator could face legal consequences

5. Risk of Detection:

- ***Identifiable by Attackers:***
  Skilled attackers may recognize a honeypot through telltale signs, such as unrealistic data, limited interaction, or anomalies in system behavior.

- ***Evasion Tactics:***
  Advanced attackers may bypass honeypots entirely by using techniques like IP reputation filtering or carefully probing systems.

6. Limited Effectiveness Against Insider Threats:

Honeypots are primarily designed to detect external threats. They are less effective in identifying malicious insiders who already have legitimate access to systems.

7. Data Overload and False Positives:

- ***Large Volumes of Data:***
  Honeypots, especially high-interaction ones, can generate significant amounts of data, making it challenging to analyze and extract actionable insights.

- ***Non-Malicious Activity:***
  Some activities captured by honeypots might not be malicious, leading to false positives that require further investigation.

8. Deployment Complexity:

- ***Integration with Existing Systems:***
  Ensuring that a honeypot does not interfere with legitimate network operations can be complex.

- ***Placement Strategy:***
  Deploying a honeypot in the wrong place (e.g., an isolated network segment) may result in it being ignored by attackers.

9. Limited Longevity:

   Once attackers recognize the presence of a honeypot, they may avoid it or share its location with others, reducing its long-term effectiveness.

10. Cost Considerations:

- ***High Cost for High-Interaction Systems:***
  Advanced honeypots that mimic real environments can be expensive to deploy and maintain, making them less accessible to smaller organizations.

Mitigating Challenges:

To address these limitations:

- Combine honeypots with other security measures for a layered defense.

- Regularly update and test honeypots to ensure effectiveness.

- Clearly define the scope and purpose of deployment.

- Adhere to legal and ethical guidelines when monitoring and analyzing data.

By understanding and managing these limitations, honeypots can be an effective part of a broader cybersecurity strategy.

Bait Tactics

Bait Tactics Bait tactics involve the use of specific strategies to lure attackers into engaging with the honeypot. Examples include exposing known vulnerabilities, placing fake data, or using social engineering tactics to attract attackers.

Good vs Bad Honeypots Good Honeypots

Effective honeypots are well-designed, strategically placed, and provide useful data. Bad Honeypots: Poorly configured honeypots can be easy to detect and fail to provide relevant data.

Conclusion

Honeypots represent a critical component of modern cybersecurity strategies, serving as both a defensive and investigative tool. By actively engaging with attackers, honeypots allow organizations to disrupt potential threats, gather valuable intelligence, and refine their overall security posture. They bridge the gap between traditional passive defenses and proactive threat hunting, offering a dynamic solution to the ever-evolving landscape of cyber threats.

Despite their numerous benefits, honeypots are not without challenges. Effective deployment requires careful planning, ongoing maintenance, and adherence to ethical and legal considerations. Organizations must integrate honeypots within a comprehensive security framework, combining them with tools such as firewalls, intrusion detection systems, and endpoint protections for a robust defense.

The future of honeypots lies in their continued innovation and adaptation to mixing technologies, such as AI & machine learning. These advancements and benefits promise to make honeypots more resilient, intelligent, and capable of addressing complex cyber threats. As cybercriminals grow more sophisticated, the role of honeypots will undoubtedly expand, cementing their place as a cornerstone of effective cybersecurity strategies.

References

- *The History of Honeypots - Honeypots: Tracking Hackers [Book]*

- *What Is a Honeypot? Meaning, Types, Benefits, and More | Fortinet*

- *What is Honeypot? - GeeksforGeeks*

- *What is Honeypot? Working, Types & Benefits*

- ***The Use of Deception Techniques: Honeypots and Decoys Paper (a study by Fred Cohen).***