

Assignment 2.1: Honeypots and Deception Techniques

Joshua A. Wortz

University of San Diego

CSOL-570

Prof. Melanie Thomas

09/14/2025

Honeypots and Deception Techniques

Honeypot and deception methodologies, along with the technologies designed to implement them for proactive defense, have gained popularity in recent years. Understanding the threat landscape is one of the most fundamental components of defense, but proactive methods can be used to catch malicious actors earlier in an attack chain.

Traditional defenses such as firewalls and antivirus software are largely reactive, waiting for indicators of compromise before alerting defenders. Honeypots, by contrast, allow defenders to proactively observe malicious behaviors, making them a vital part of modern layered defense strategies (Diogenes & Ozkaya, 2022).

Defining Honeypot and Deception Methodologies

A honeypot is a security resource whose value lies in being probed, attacked, or compromised (HHS Cybersecurity Program, 2020). These systems are designed to appear as legitimate targets to lure attackers away from critical assets and allow defenders to study their tactics, techniques, and procedures (TTPs).

There are three main types of honeypots:

- Honey Systems, which imitate a whole operating system and its services.
- Honey Services, which mimic specific software or protocol functions, such as an HTTP or SSH server.
- Honey Tokens, which are fake data, such as a Word document or database entry, strategically placed to alert defenders if accessed or stolen (HHS Cybersecurity Program, 2020).

For a honeypot to be effective, it must be deceptive, discoverable, interactive, and monitored, with all interactions logged and triggering an alert (HHS Cybersecurity Program, 2020).

Deception methodologies expand this concept by deliberately misleading attackers with false information about organizational assets. These tactics follow a "See-Think-Do" model: attackers must first “see” the deceptive asset, “think” it has value, and then “do” something with it that generates an alert. Whaley’s Deception Taxonomy categorizes deception as “hiding” (masking) or “showing” (mimicking) (HHS Cybersecurity Program, 2020).

Purpose and Implementation Considerations

The purpose of honeypots and deception can be viewed from both offensive and defensive perspectives. Their primary goals are research, resource exhaustion, and intrusion detection (HHS Cybersecurity Program, 2020).

From an offensive research perspective, honeypots gather threat intelligence by observing attacker behavior. For example, defenders can learn how an adversary uses a tool like Metasploit by observing their interaction with a vulnerable system (Tanner, 2019).

Resource exhaustion aims to waste attackers’ time by engaging them with decoy systems instead of tangible assets, buying defenders valuable time to detect and respond (HHS Cybersecurity Program, 2020).

The defensive goal is high-confidence intrusion detection. Since legitimate users should not interact with honeypots, any contact reliably indicates malicious activity (HHS Cybersecurity Program, 2020).

Effective implementation requires careful planning:

- Provisioning: Choose between low-interaction honeypots (easier to maintain) and high-interaction honeypots (more detailed but riskier). For instance, canary tokens act as low-risk tripwires.
- Monitoring: Honeypots must integrate with existing log servers and provide data that can be filtered and analyzed (HHS Cybersecurity Program, 2020).
- Reacting: Organizations should establish incident response playbooks, including defined roles, communication paths, and mitigation strategies.

Business Implications and Operationalization

Honeypots and deception bring certain risks:

- Pivot Points: High-interaction honeypots could be abused as a launchpad if not isolated.
- Detection: Advanced attackers may recognize a honeypot, though valuable intelligence can still be gathered (HHS Cybersecurity Program, 2020).
- Legal/Policy Challenges: Deploying deception must align with applicable laws and organizational policies. Tanya Janca highlights that some organizations avoid deception technologies due to perceived risks (Carey & Jin, 2020).

- False Sense of Security: Honeypots should complement, not replace, existing defenses.

Misconfigurations can introduce vulnerabilities (HHS Cybersecurity Program, 2020).

To operationalize deception securely, organizations should:

- Isolate Honeypots: Run high-interaction honeypots in segmented environments.
- Layer Defenses: Use honeypots alongside IDS/IPS, endpoint detection, and firewalls.
- Formalize Policies: Develop compliance-aligned policies and embed security goals into performance metrics.
- Educate and Communicate: Train staff on security awareness and frame deception strategies in terms of business value, such as customer trust and resilience.

Case Studies of Honeypot Use

Honeypots have been successfully deployed to track real-world cyber threats. For instance, the WannaCry ransomware outbreak highlighted how unpatched SMB vulnerabilities were exploited at scale. Researchers using honeypots were able to collect malware samples, study propagation methods, and provide actionable intelligence to organizations worldwide (Diogenes & Ozkaya, 2022).

Another example is the use of IoT honeypots to monitor Mirai botnet activity. By emulating vulnerable IoT devices, defenders could track command-and-control servers and better understand how attackers built large botnets for distributed denial-of-service (DDoS) attacks. These insights informed patching strategies and security awareness for manufacturers and consumers alike.

Ethical and Legal Considerations

The deployment of honeypots raises ethical and legal questions. The U.S. Computer Fraud and Abuse Act (CFAA) prohibits unauthorized access to systems, making it essential that organizations deploying honeypots carefully scope their use and gain explicit authorization (Tanner, 2019). Misuse or misconfiguration could expose defenders to liability.

From an ethical standpoint, defenders must balance deception with transparency. While honeypots aim to mislead attackers, they should not endanger legitimate users or create undue risk. Organizations must document their intent, isolate honeypots from production systems, and ensure all stakeholders understand the limitations and goals of deception strategies (Carey & Jin, 2020).

Future of Deception Technologies

As attackers evolve, so too must deception strategies. Emerging approaches include AI-driven adaptive honeypots that can change their behavior in response to attacker actions, making them harder to detect. Integration with frameworks like MITRE ATT&CK also helps map adversary tactics more precisely to defensive measures (Diogenes & Ozkaya, 2022).

Cloud-native deception platforms are another trend, where honeypots are deployed elastically within virtualized and containerized environments. This enables defenders to scale deception alongside their infrastructure. Looking ahead, deception technologies may become integral to Zero Trust security models, reinforcing the principle of “never trust, always verify.”

References

Carey, M. J., & Jin, J. (2020). *Tribe of hackers blue team*. Wiley.

Diogenes, Y., & Ozkaya, E. (2022). *Cybersecurity – Attack and Defense Strategies* (3rd ed.). Packt Publishing.

HHS Cybersecurity Program, Office of Information Security. (2020, October 22). *Using honeypots for network intrusion detection*. <https://www.hhs.gov/sites/default/files/using-honeypots-network-intrusion-detection.pdf>

Tanner, N. H. (2019). *Cybersecurity blue team toolkit*. Wiley.