honey pots & decoys

Presented by
Djedouani med abdallah.
Khaldi med louai.
Haoues aymen.

Nov 2025

Content

Now 2025

Concept of cyber deception →

Cyber deception is a proactive security and defense tactic where you deliberately mislead, confuse and manipulate attackers by giving them false information , fake systems and traps , making it harder for the them to succeed and easier for you to detect them .

Attacker Evasion : ⟶

all the techniques attackers use to avoid being detected by security systems such as firewalls, IDS, IPS, antivirus, SIEM, honeypots, and decoys. basically: how attackers hide themselves. and here’s some of the most common evasion techniques:

- **obfuscation**
- **spoofing**
- **fragmentation**
- **living off the land**
- **slow and low**
- **encrypted channels**
- **manipulating logs**
- **file malware**

Defender Counter-Evasion

all the techniques used by defenders (blue team) to detect, block, and neutralize attackers who are trying to hide or evade detection. basically stopping attackers from hiding.

- **Deep Packet Inspection**
- **Behavioral Analysis**
- **Deception Technology**
- **Threat Intelligence**
- **Memory Monitoring**
- **Sandboxing**
- **TLS/SSL Inspection**
- **Rate-Limiting**

Honeypots : defenition

A honeypot is a cybersecurity mechanism that uses a manufactured attack target to lure cybercriminals away from legitimate targets. They also gather intelligence about the identity, methods and motivations of adversaries.

Honeypots:types and uses (purpose based classification)

research honeypots:

designed to collect in-depth information about attacker behavior, advanced techniques, and new threat patterns. They provide a high-resolution view of how adversaries operate in the wild.

prouduction honeypots:

the most commonly deployed type of honeypot. Its primary purpose is to operate inside a company’s real production network and help detect malicious activities as early as possible.

Honeypots:types and uses (complexity based classification)

low-interaction

simulate only a limited set of services or functionalities, They require minimal system resources and are straightforward to deploy and maintain

high-interaction

simulate full systems, often with multiple services, databases, and applications.

low-interaction

A more advanced classification is deception technology, which extends traditional honeypots using: AI, ML, automation.

Honeypots:types and uses

(activity based classification)

Email Trap / Spam Trap

a honeypot that uses fake, hidden email addresses placed in areas only visible to automated crawlers .

Decoy Database

a fake, intentionally vulnerable database designed to attract attackers.

Malware honeypot

mimics a software or an API in an attempt to draw out malware attacks in a controlled environment.

low-interaction

designed to trap web crawlers by creating web pages and links only accessible to automated crawlers.

Decoyos : defenition →

A decoy is a fake digital asset intentionally planted inside a system or network to mislead attackers, divert them away from real resources, and trigger early detection when accessed.

Decoys are designed to look real, feel real, and behave like legitimate assets, but have no operational value to the organization.

Decoys : types and uses

breadcrumbs

Fake Credentials – Fake login details or API keys left to lure attackers into revealing themselves.

Deceptive Services

Fake services or ports that appear real but only exist to detect scanning or intrusion.

Canary Files

Files that trigger alerts when accessed or moved, without being a full honeypot system.

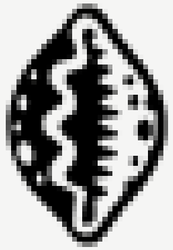
Decoy Endpoints

Fake user accounts or devices on a network that signal suspicious access attempts.

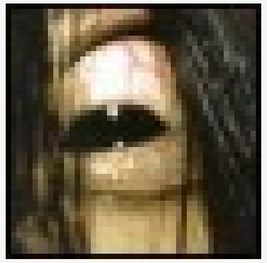
honeypots vs decoys

	honeypot	decoy
purpose	capture and study attacks	distract and mislead attackers
interaction	high/ medium/low	very low
complexity	meduim to high	very low
logging	extensive	minimal
risk	higher	very low

open source solutions



cowrie



kippo

Dionaea

T-pot

commercial solutions

Thinkst Canary

cybertrap

sentinelone

shoadowPlex

honeypots

R

- Attacker can use it as a pivot
- Legal and ethical issues
- High-interaction honeypots are dangerous

L

- They only detect what interacts with them
- Limited coverage
- Requires configuration & maintenance
- Can be fingerprinted

decoys

R

- Maintenance effort
- Attackers may use decoys for reconnaissance
- If placed badly, they alert legitimate users

L

- Very low interaction
- Easy to identify
- Requires large-scale deployment
- Skilled attackers ignore them

conclusion:

Honeypots and decoys help detect and analyze cyber attacks while diverting attackers from real assets. They provide valuable threat intelligence and improve overall security posture.
However, they require careful management to avoid misuse and minimize risks.

Thank you

For your attention