Honeypots

A honeypot **is a decoy system or service designed to mimic a real system within a network to attract and detect attackers**. The primary purpose of a honeypot is to monitor and record the activities of potential intruders, allowing security teams to understand attack methods, gather intelligence, and improve defenses without exposing critical systems. Honeypots **do not contain real data or services but are configured to look authentic to attackers**.

Types of Honeypots:

1. **Low-Interaction Honeypots**: Simulate a limited set of services and are less complex, designed to **detect basic attack patterns and reconnaissance activity**.
2. **High-Interaction Honeypots**: Provide full, realistic services (like web servers, SSH, databases) to **observe a wide range of attacker behaviors**. These honeypots allow the attacker to interact with what appears to be a genuine system, giving security teams more detailed insights into their tactics and tools.

Canary Tokens:

- Canary tokens are **a specific type of honeypot technique used to detect when attackers access sensitive or decoy data**. A canary token is **a trigger that silently alerts the security team when it is accessed, modified, or used in any way by an unauthorized entity**.
- How Canary Tokens Work:
    - Canary tokens can take many forms, such as:
        - **Decoy credentials**: Fake login credentials stored in an accessible place. If an attacker attempts to use these credentials, the system immediately alerts security teams.
        - **Fake files**: A file (e.g., a Word document or PDF) that sends a notification when opened.
        - **DNS Canary Tokens**: A token linked to a specific DNS name that, if queried, triggers an alert.
    - Canary tokens **allow organizations to detect early-stage breaches**, such as when attackers are performing reconnaissance or attempting lateral movement within the network.

Example: A decoy file named passwords.txt is placed in a folder where an attacker might search for credentials. If the file is opened, the token inside the file triggers an alert to the security team, notifying them of suspicious activity.

Dummy Internal Service / Web Server:

- A dummy internal service or web server is a honeypot set up inside the organization's network to mimic real services (e.g., web servers, database servers) that are used by attackers during reconnaissance or lateral movement.
- Purpose:
    - These decoy services are configured to appear vulnerable or valuable to an attacker. They allow security teams to:
        - Monitor Traffic: Track how attackers interact with the dummy service, what tools they use, and what vulnerabilities they try to exploit.

        - Detect Attackers: When attackers attempt to access or compromise the decoy service, security teams can observe these actions in real time.
        - Study Attack Patterns: By monitoring how attackers interact with the dummy service, organizations can better understand the latest attack methods and develop stronger defenses.
    - Example: A fake internal web server running a dummy e-commerce site or a fake database that appears to hold sensitive information. These honeypots attract attackers who might be looking for internal resources to exploit or steal data.

How Honeypots and Canary Tokens Help:

- **Early Detection**: Honeypots and canary tokens can detect attackers early in the attack chain, often during the reconnaissance phase, before they reach critical systems.
- **Minimal False Positives**: Since honeypots are not meant to be accessed by legitimate users, any interaction with them is almost certainly malicious, resulting in fewer false positives compared to other detection methods.
- **Gathering Intelligence**: Honeypots allow organizations to gather valuable intelligence about an attacker's methods, tools, and behavior, which can be used to strengthen security defenses.
- **Low-Cost Deception**: Honeypots and canary tokens are often low-cost methods of deception and can be highly effective in confusing and deterring attackers.

Summary:

- Honeypots are decoy systems designed to attract attackers, providing a way to monitor and record their actions without exposing real assets. These systems can simulate internal services or web servers.
- **Canary tokens are lightweight honeypot triggers** that alert security teams when accessed, used in decoy files, fake credentials, or DNS queries to detect attackers during early stages of a breach.
- Both honeypots and canary tokens are essential tools for early detection, monitoring attacker behavior, and improving security defenses without risking real assets.