4.6 HONEYPOTS

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.

A honeypot can be modeled after any digital asset, including software applications, servers or the network itself. It is intentionally and purposefully designed to look like a legitimate target, resembling the model in terms of structure, components and content. This is meant to convince the adversary that they have accessed the actual system and encourage them to spend time within this controlled environment.

The honeypot serves as a decoy, distracting cybercriminals from actual targets. It can also serve as a reconnaissance tool, using their intrusion attempts to assess the adversary's techniques, capabilities and sophistication.

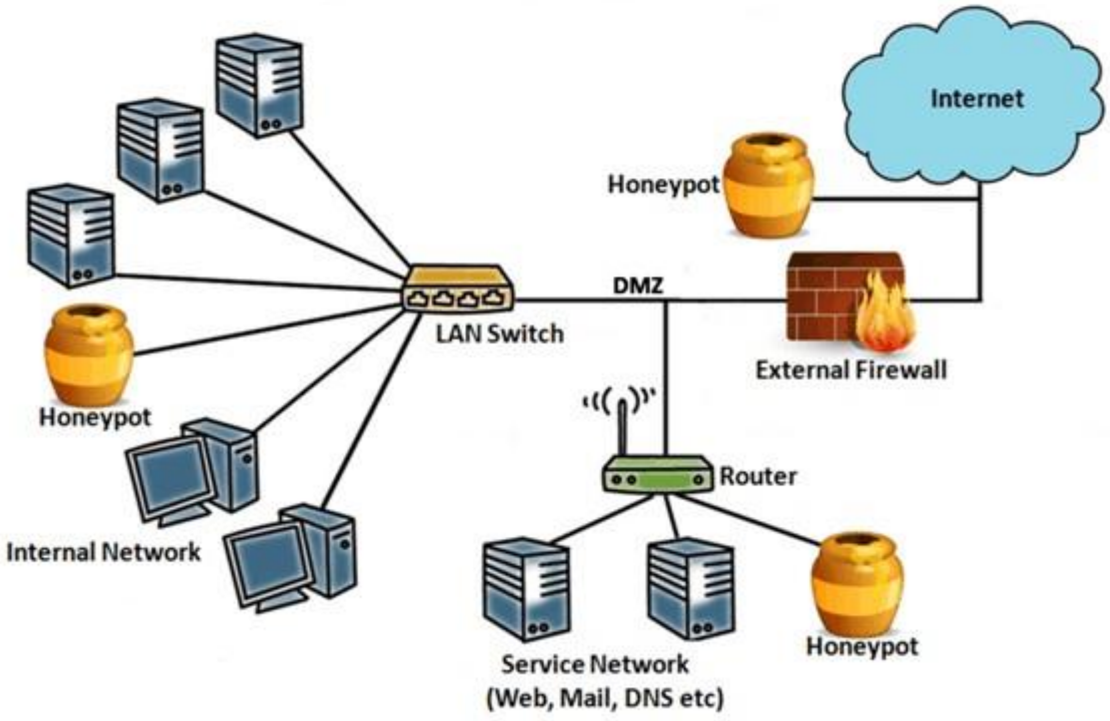
The intelligence gathered from honeypots is useful in helping organizations evolve and enhance their cybersecurity strategy in response to real-world threats and identify potential blind spots in the existing architecture, information and network security.

Honeypot is a network-attached system used as **a trap for cyber-attackers** to detect and study the tricks and types of attacks used by hackers. It acts as a potential target on the internet and informs the defenders about any unauthorized attempt to the information system.

Honeypots are mostly used by large companies and organizations involved in cybersecurity. It helps cybersecurity researchers to learn about the different type of attacks used by attackers. It is suspected that even the cybercriminals use these honeypots to decoy researchers and spread wrong information.

The **cost of a honeypot** is generally **high** because it requires specialized skills and resources to implement a system such that it appears to provide an organization's resources still preventing attacks at the backend and access to any production system.

A **honeynet** is a combination of two or more honeypots on a network.



Types of Honeypots:

Honeypots are classified based on their deployment and the involvement of the intruder. Based on their deployment, honeypots are divided into :

1. **Research honeypots-** A research honeypot is designed to collect information about the specific methods and techniques used by adversaries and what possible vulnerabilities exist within the system in reference to such tactics. Research honeypots are typically more complex than production honeypots. They are often used by government entities, the intelligence community and research organizations to get a better sense of the organization's security risks.

2. **Production honeypots-** The production honeypot is the most common honeypot type. This decoy is used by businesses to collect information and intelligence about cyberattacks within the production network. This may include IP addresses, intrusion attempt time and dates, traffic volume and other attributes.

   Production honeypots are relatively simple to design and deploy, but they are less sophisticated than research honeypots in terms of the intelligence produced. They are most commonly used by corporations, private companies and even high-profile individuals, such as celebrities, political figures and business leaders.

3. Based on interaction, honeypots are classified into:

1. **Low interaction honeypots:** Low interaction honeypots gives very little insight and control to the hacker about the network. It simulates only the services that are frequently requested by the attackers. The main operating system is not involved in the low interaction systems and therefore it is less risky. They require very fewer resources and are easy to deploy. The only disadvantage of these honeypots lies in the fact that experienced hackers can easily identify these honeypots and can avoid it.
2. **Medium Interaction Honeypots:** Medium interaction honeypots allows more activities to the hacker as compared to the low interaction honeypots. They can expect certain activities and are designed to give certain responses beyond what a low-interaction honeypot would give.
3. **High Interaction honeypots:**A high interaction honeypot offers a large no. of services and activities to the hacker, therefore, wasting the time of the hackers and trying to get complete information about the hackers. These honeypots involve the real-time operating system and therefore are comparatively risky if a hacker identifies the honeypot. High interaction honeypots are also very costly and are complex to implement. But it provides us with extensively large information about hackers.

Types of Honeypots

Honeypots can also be broken down by the type of activity they detect.

Email trap or spam trap

An email or spam trap will implant a fictitious email address in a hidden field that can only be detected by an automated address harvester or site crawler. Since the address is not visible to legitimate users, the organization can categorize all correspondence delivered to that inbox as spam. The organization can then block that sender and its IP address, as well as any messages that match its content.

Decoy Database

A decoy database is an intentionally vulnerable fictitious data set that helps organizations monitor software vulnerabilities, architecture insecurities or even nefarious internal actors. The decoy database will gather information about injection techniques, credential hijacking or privilege abuse used by an attacker that can then be built into system defenses and security policies.

Malware Honeypot

A malware honeypot mimics a software app or an application programming interface (API) in an attempt to draw out malware attacks in a controlled, non-threatening environment. In doing so, the infosec team can then analyze the attack techniques and develop or enhance anti-malware solutions to address these specific vulnerabilities, threats or actors.

Spider Honeypot

Similar to the spam honeypot, a spider honeypot is designed to trap web crawlers, sometimes called spiders, by creating web pages and links only accessible to automated crawlers. Identifying these spiders can help organizations understand how to block malicious bots, as well as ad-network crawlers.

Advantages of honeypot:

1. Acts as a rich source of information and helps collect real-time data.
2. Identifies malicious activity even if encryption is used.
3. Wastes hackers' time and resources.
4. Improves security.

Disadvantages of honeypot:

1. Being distinguishable from production systems, it can be easily identified by experienced attackers.
2. Having a narrow field of view, it can only identify direct attacks.
3. A honeypot once attacked can be used to attack other systems.
4. Finger printing(an attacker can identify the true identity of a honeypot).