JIMMA UNIVERSITY

JIMMA INSTITUTE OF TECHNOLOGY

FACULTY OF COMPUTING AND INFORMATICS

DEPARTMENT OF SOFTWARE ENGINEERING

ASSIGNMENT OF FUNDAMENTAL SOFTWARE SECURITY

Name	USMAEL TAJU AHMED
Id	RU1061/14
Section	2

Submitted to Mr Ermias T

Honeypot

A honeypot is a cybersecurity method that uses a simulated attack target to distract criminals(attackers) away from authentic systems. These methods can simulate a variety of digital assets, including software applications, servers, and even a whole network. Organizations utilize this data to improve their cybersecurity methods and discover potential weaknesses in their current infrastructure.
It 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 at the information system. Honeypots are mostly used by large companies and organizations involved in cyber security. It helps cybersecurity researchers to learn about the different types of attacks used by attackers. It is suspected that even 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 while still preventing attacks at the backend and access to any production system.

Types of Honeypot

Honeypots are classified based on their deployment and the involvement of the intruder.

1. Based on their deployment, Honeypots are divided two.

Research honeypots: These are used by researchers to analyze hacker attacks and deploy different ways to prevent these attacks.

Production honeypots: Production honeypots are deployed in production networks along with the server. These honeypots act as a frontend trap for the attackers, consisting of false information and giving time to the administrators to improve any vulnerability in the actual system.

2. Based on interaction, honeypots are classified three

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.

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.

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.

How do Honeypots Work?

Detection and Monitoring: By analyzing the activity on honeypots, security teams gain insights into attack techniques, patterns, and vulnerabilities. They can identify new threats or zero-day exploits.

Diversion: Honeypots divert attackers away from critical systems. Instead of compromising actual assets, cybercriminals waste time and resources on the decoy.
Research and Analysis: Researchers study attacker behavior, tactics, and tools by observing honeypot interactions. This knowledge informs better defense strategies.
Early Warning: If an attacker targets a honeypot, it triggers an alert. Security teams can respond promptly to potential threats

Advantages of Honeypot

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

Disadvantages of Honeypot

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

Conclusion

Honeypots are effective cybersecurity technologies for detecting, analysing, and mitigating cyber attacks. They help organisations strengthen their security measures by replicating hackers' targets. Despite their high cost and associated risks, honeypots play an important role in diverting attackers away from real assets and improving overall security.