HONEYPOT: STUDY ASSIGNMENT

NAME: Megha

CLASS: BE COMP 3

PRN: F21113029

What is Honeypot?

A 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 at the information system. Honeypots are mostly used by large companies and organizations involved in cybersecurity. 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 into

- **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.

3. Based on interaction, honeypots are classified into

- **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).

What is Honeynet?

A honeynet is made up of two or more honeypots connected via a network. Having a linked network of honeypots can be beneficial. It allows organisations to trace how an attacker interacts with a single resource or network point while also monitoring how a hacker moves between network points and interacts with numerous points at the same time. The goal is to

induce hackers to believe that they have successfully breached the network. Having more false network destinations makes the arrangement appear more realistic.

Example scenario: database attack

A power company can set up a fake Microsoft SQL server that appears to contain a database of the locations of all the plants it uses to source the power it sells to customers.

So suppose the power company has eight hydroelectric plants, one nuclear power plant, 10 solar farms, and two coal-burning power plants that all provide power to the people the company serves. Network admins can create a fake database, host it on an SQL server, make it relatively easy to hack into, and then use this honeypot to see how hackers try to steal the information. Of course, the names of the power plants, and especially their geolocations, are all false.

In many cases, the IT team will create a system that closely parallels their real network setup. In this way, if hackers are able to get in, they can identify vulnerabilities in their actual setup.

It is important to keep in mind that honeypots in network security are designed based on your IT team's objectives. Consequently, honeypot security setups can vary drastically from one organization to another.

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.