Subject: Information and Communication Technology (ICT)
Topic: Honeypots
Lesson: Three
Teacher: Chinyere **.**E. Ikpah
Class: Senior Secondary Class 2
Duration: 80 Minutes

Objectives

At the end of this lesson, students should be able to:

- Define honeypot,
- Explain classification of honeypot,
- Explain types of honeypots,
- Explain types of honeypot technologies,
- Explain benefits of honeypots in network security.

What is Honeypot?

A honeypot is a network-attached system set up as a decoy to lure cyber attackers and detect, deflect and study hacking attempts to gain unauthorized access to information systems.

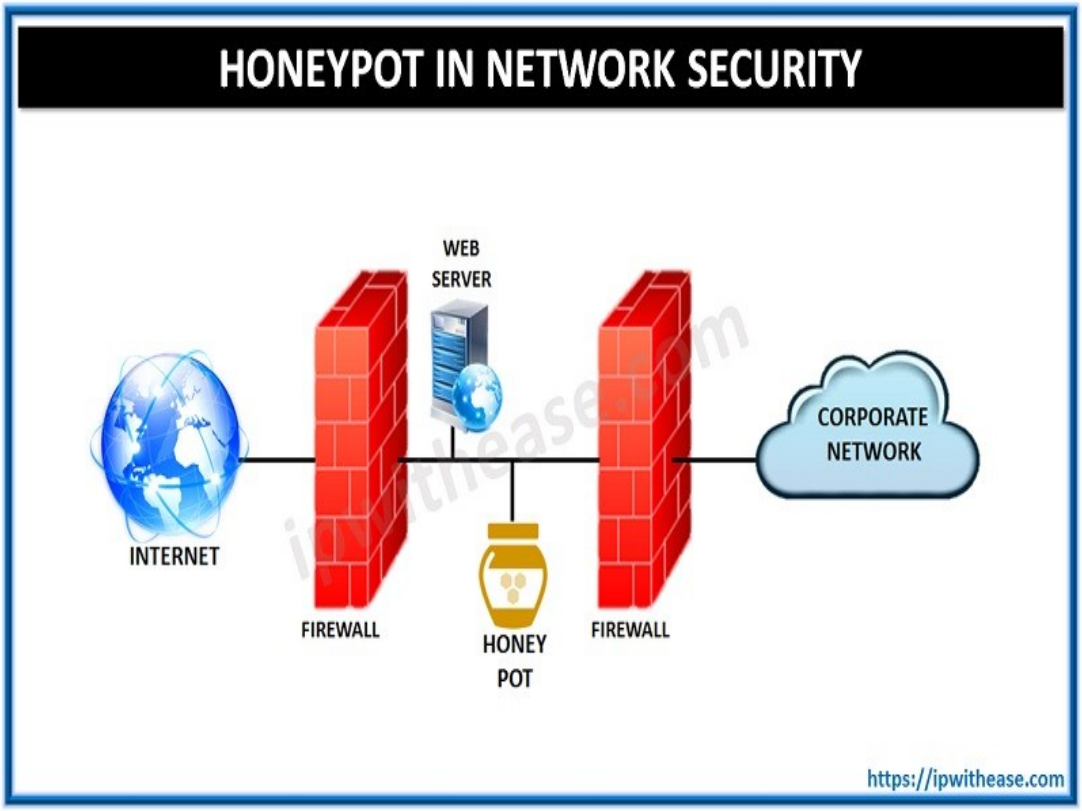

Fig 11: Overview of honeypot in network security

Honeypot can be made with a range of complexities on the grounds of what is actually required by your organization.
Honeypots help us in tracing an early sign of attack, what type of information is vulnerable, what are the details of the attackers and what are the methods used by them? Honeypots are well monitored and actually do not contain sensitive data. It helps in analysing TTPs (tools, tactics and procedures) of the attackers and accumulates legal and forensic evidence without putting the real network security at stake.

How a Honeypot Work

Honeypot is a system to collect intelligence. Honeypots are usually located behind the firewall. Honeypots are mainly used to simulate a variety of services and holes, to induce the occurrence of various attacks, attack data. When an intruder tries to enter the system with a fake identity, the administrator system will be notified. According to Open Web Application Security Project (OWASP) some top attacks

recorded were SQL injection and XSS. When someone tries to enter the system, a log is generated about all the entries. Even though the intruder succeed in entering the system and captures the data from the database, we can fool them by providing fake data, this is done by honeypot, but intruder will not be aware about this fake information. So by this we can save our system and fool intruders. At the same time the logs will be created, so that all the data about attacker are recorded like system IP, attack type, attack pattern, available footprints etc., and attack method for the evidence which can be used for further actions.

Classification of Honeypots

Honeypots can be classified based on the purpose as **Research honeypot** and **Production honeypot**.

Research honeypot: Research honeypots are basically used for learning new methods and tools of attacks. Research honeypots are used to gather intelligence on the general threats organizations may face, which gives the organization a better protection against those threats. Its main goal is to gain info about the way in which the attackers progress and performs lines of attacks. Research honeypots are complex to build, deploy and manage. They are basically used by organizations like universities, governments, the military and intelligence systems to learn more about threats. Research honeypots provides a strong platform to study cyber threats and forensic skills.

Production honeypot: Production honeypots are simply aimed to protect the network. Production honeypots are easy to build and deploy, as they require very less functionalities. They protect the system by detecting attacks and giving alerts to administrators. It is typically used within an organization environment to protect the organization.

As the job role indicates, **research honeypots** are more complex and carry additional forms of data files in comparison to **production honeypots**.

Honeypot Types

- **Pure Honeypot:** A full-scale production replication system that can run on different servers. It has comprehensive sensors and carries dummy *"confidential"* data and user details.

- **High-Interaction Honeypot**: It is used by the security analyst to observe attacker's techniques and behaviour pattern. These types of honeypot are quite resource-intensive and demand more maintenance, but can deliver worthwhile findings.

  This is the most advanced honeypot. This type of honeypot has very higher level of interaction with the intrusive system. It gives more realistic experience to the attackers and gathers more information about intended attacks; this also involves very high risk of capturing of whole honeypot. High-interaction honeypot are most complex and time consuming to design and manage. High-interactive honeypots are more useful in the cases, where we want to capture the details of vulnerabilities or exploits that are not yet known to the outside world. This honeypots are best in the case of "0-Day attacks". Ex: Honeynets: which are typically used for research purpose.

- **Mid-Interaction Honeypot**: They do not possess own operating system, and primarily used to confuse the attackers in order to buy some time for the security team to react to the breach.

  These are also known as mixed-interactive honeypots. Medium-interaction honeypots are slightly more sophisticated than low-interaction honeypots, but are less sophisticated than high-interaction honeypots. It provides the attacker with a better illusion of the operation system so that more complex attacks can be logged and analysed. Ex: Honeytrap: it dynamically creates port listeners based on TCP connection attempts extracted from a network interface stream, which allows the handling of some unknown attacks

- **Low-Interaction Honeypot**: This form of honeypot in network security is widely deployed while creating a production environment. It is used for advanced warning spotting mechanism. They are quite simple to deploy and maintain.

  These types of honeypots have the limited extend of interaction with external system. FTP is the example of this type of honeypot. There is no operation system for attackers to interact with, but they implement targets to attract or detect attackers by using software to emulate features of a particular operating system and network services on a host operation system. Main advantage of this type of honeypot is that, it is very easy to deploy and maintain and it does not involve any complex architecture. With this advantage there is also some drawback of this system. That is, it will not respond accurately to exploits. This creates the limitation in ability to aid in discovering new vulnerabilities or new attack patterns. Low-interactive honeypots are a safer and easy way to gather info about the frequently occurred attacks and their sources.

Types of Honeypot Technologies

Some of the key honeypot technologies are as follow-

- **Malware Honeypots:** It is known to replicate and use attack vectors to identify malware. One example is Ghost USB honeypot meant to safeguard the machine from malware spread through USB.

- **Spam Honeypots:** It is used to simulate open proxies and mail relays. It detects and blocks the large quantity of spam emails dispatched by the spammers.

- **Database Honeypots:** It helps in creating decoy databases. These types of honeypots are effective against activities like SQL injections that frequently go untraced by the firewalls.

- **Client Honeypots:** It is helpful in tracing out malicious servers that are primarily responsible for attacking clients. It functions over virtualization technology and implement a containment strategy in order to curtail the risk imposed on the research team.

- **Honeynets:** It is a single system comprising of multiple honeypots in the network security. The purpose of the honeynets is to tactically track down the motives and methods of the attacker, simultaneously containing all sorts of outbound and inbound traffic.

Benefits of Honeypot in Network Security

The following are some of the major benefits of a honeypot-

- **Ability to break/ slow attackers down:** The attackers while scanning your network always seek misconfigurations and vulnerable devices. An encounter with the honeypot renders you the chance to investigate and restrain the attack on time.

- **Unambiguous in Approach:** Honeypot does provide you with precise alert and location of the breach. It does help you out with identifying the loopholes as well as the invasion threat without scanning unnecessary locations and wasting the time.

- **Easy to Install and demand low-maintenance:** Modern honeypots are easy to download and install. They also require low-maintenance time and cost.

Summary:

In this lesson, we were able to:

A. Define honeypot.
B. Explain classification of honeypot.
C. Explain types of honeypots.
D. Explain types of honeypot technologies,
E. Explain benefits of honeypots in network security.

Evaluation:

1. The three levels of honeypot interaction are all EXCEPT

A. High level

B. Medium level

C. Low level

D. Mega level

2. What is a system designed to lure attackers?

A. Honeypot
B. Honeybee
C. Honeyboot
D. Honeypoint

3. In terms of functioning purpose, which of these is a type of honeypots?

A. Pure honeypots
B. Research honeypots
C. High interaction honeypots
D. Low interaction honeypots

4. All these are types of honeypots EXCEPT

A. High interaction honeypots
B. Medium interaction honeypots
C. Low interaction honeypots
D. Mega interaction honeypots

5. What type of honeypot technology comprises multiple honeypots in the network security?

A. Honeynets
B. Client honeypots
C. Spam honeypots
D. Malware honeypots