SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING-IOT Including CS&BCT

COURSE NAME : 19SB402 NETWORKING AND CYBERSECURITY

II YEAR / IV SEMESTER

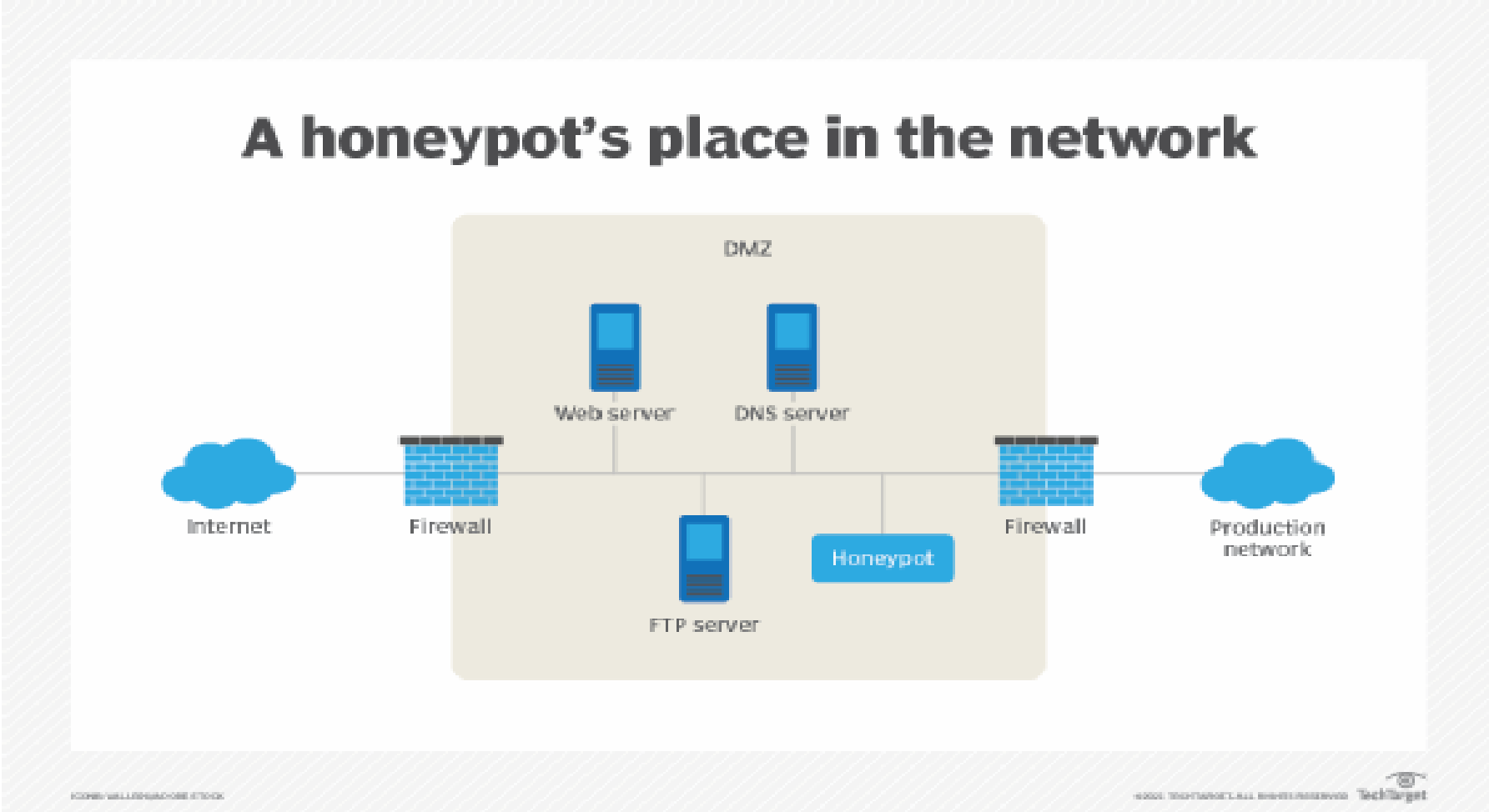
Unit IV- SECURITY ELEMENTS

Topic : Honey Pots

Honeypot

- **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.
- 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.

Honeypot


A honeypot's place in the network
DMZ
Web server
DNS server
Internet
Firewall
Honeypot
Firewall
Production network
FTP server

Types of Honeypot

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

Based on **their deployment, honeypots** are divided into :

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

2.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.

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.

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.

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.

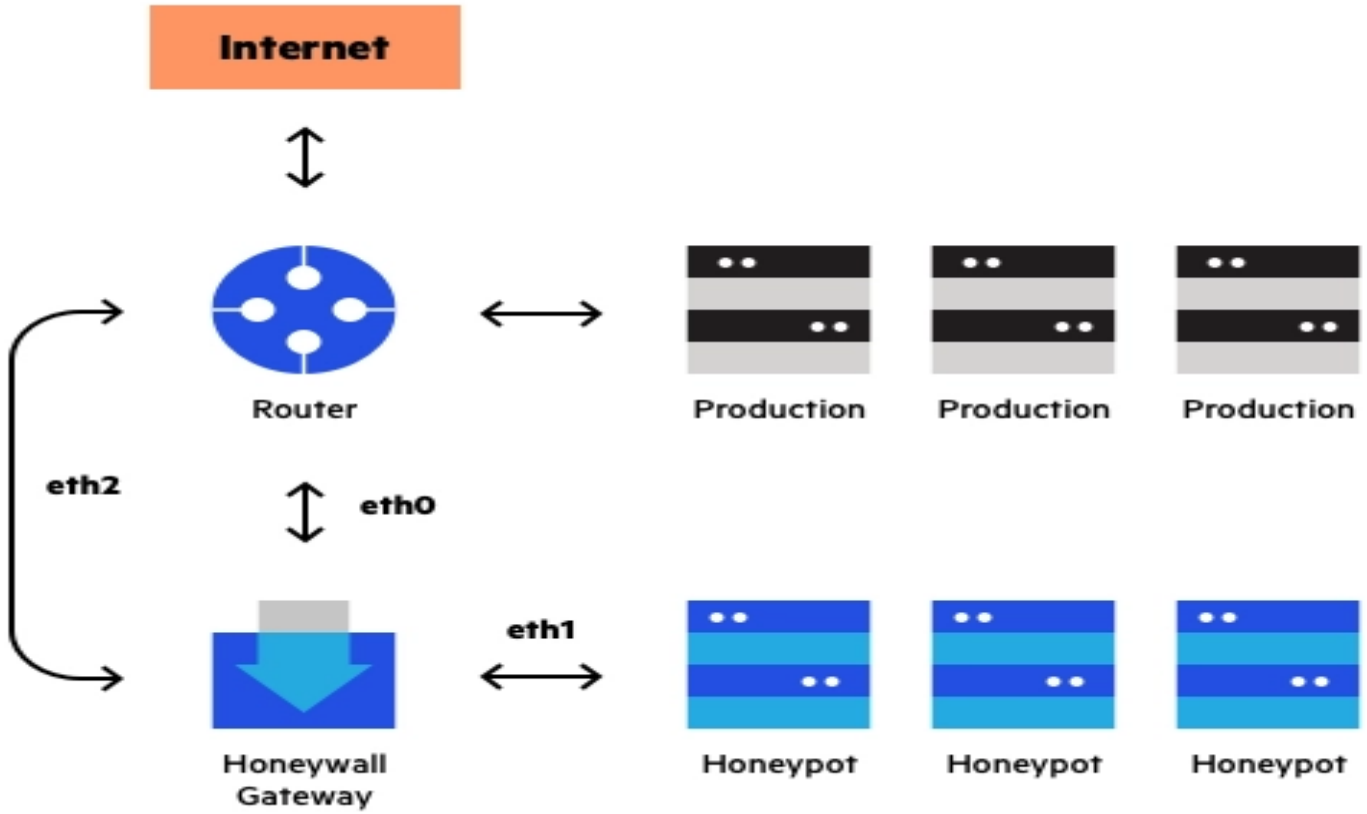
2.Having a narrow field of view, it can only identify direct attacks.

3.A honeypot once attacked can be used to attack other systems.

4.Fingerprinting(an attacker can identify the true identity of a honeypot).

Honey net

- A **honeynet** is a **combination of two or more honeypots** on a network.
- A honeynet is a decoy network that contains one or more honeypots. It looks like **a real network and contains multiple systems** but is hosted on one or only a few servers, each representing one environment.
- For example, a Windows honeypot machine, a Mac honeypot machine and a Linux honeypot machine.


Internet
Router
Production
Production
Production
eth2
eth0
eth1
Honeywall
Gateway
Honeypot
Honeypot
Honeypot

Any Query????

Thank you……