WIRELESS INTRUSION PREVENTION SYSTEM

MODULE 2

INTRODUCTION

- Recently, most use of wireless networks, network security has become **more important** than ever before. Therefore, understanding and deploying effective wireless **network protection measures have become crucial.**

- WIPS security solution is designed to monitor, **protect, and prevent malicious attacks** and threats to wireless networks. Additionally, WIPS focuses on **monitoring and responding** to abnormal activities in wireless networks.

- WIPS security solution is designed to monitor, **protect, and prevent malicious attacks** and threats to wireless networks. Additionally, WIPS focuses on **monitoring and responding** to abnormal activities in wireless networks.

How does WIPS work?

WIPS ensures the security of wireless networks through a series of advanced technologies:-

- **Network Monitoring**
- **Wireless Device Classification**
- **Threat Detection**
- **Defense and Response**
- **Data Analysis and Reporting**
- **Automation and Integration**
- **Policy Management and Updates**
- **Location Tracking**

What Threats Can WIPS Defend Against?

WIPS has various threat defense strategies and can defend against, but not limited to, the following threats:

- **Unauthorized Access Points**
- **Malicious Attacks and Network Penetration**
- **Illegal Associations and Bandwidth Abuse**
- **Data Leak Prevention**
- **Authentication and Encryption Vulnerabilities**
- **Unsafe Configurations**
- **Software Vulnerabilities and Configuration Errors**

CONTT..

- **Client Risks**
- **Evil Twin Attack**
- **Rogue Access Point**
- **De-authentication Attack**

CONTT..

WIPS provides an additional layer of protection, helping to ensure the security of the network environment and guarantee data protection.

a) **Security Enhancement-**

b) **Network Performance**

c) **Reduced Business Disruptions**

d) **Ease of Management**

HONEYPOT-

A cyber honeypot works as by baiting a trap for hackers.

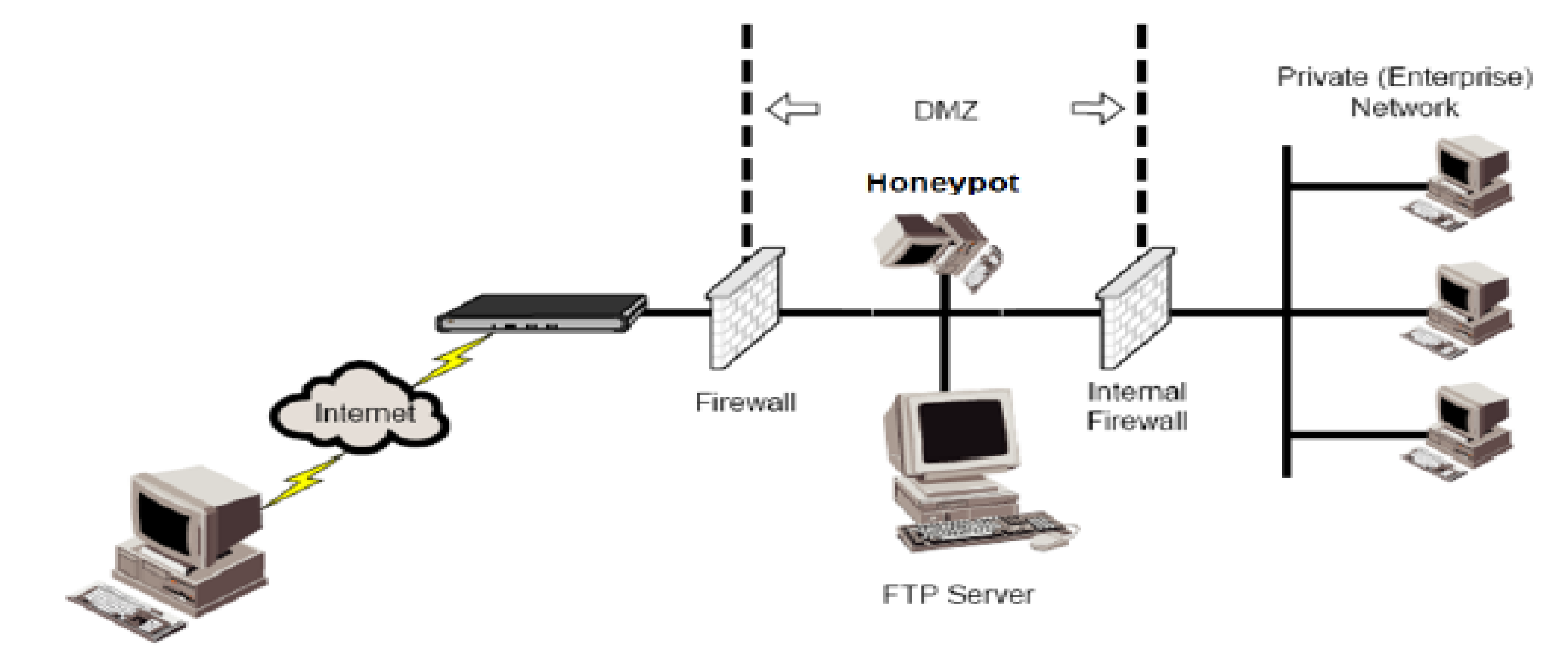
It's a sacrificial computer system that’s intended to attract cyber-attacks.

It mimics a target for hackers, and uses their **intrusion attempts to gain information** about cybercriminals and the **way they are operating or to distract them from other targets.**

Often, an enemy spy is compromised by a honey trap and then forced to hand over everything he/she knows.

Honeypot

A honeypot is a computer typically located in a DMZ that is loaded with software and data files that appear to be authentic, yet they are actually imitations of real data files.



How it works?

- The honeypot looks like a **real computer system**, with applications and data, **fooling cybercriminals** into thinking it's a **legitimate target.**
- For example, a honeypot could mimic a company's **customer billing system** - a frequent target of attack for criminals who want to **find credit card numbers**.
- Once the hackers are in, they can be tracked, and their **behavior assessed for clues** on how to make the **real network more secure.**

- Honeypots are made attractive to attackers by building in **deliberate security vulnerabilities.**
- For instance, a honeypot might have ports that respond to a **port scan or weak passwords.**
- Vulnerable ports might be **left open to entice attackers into the honeypot environment,** rather than the **more secure live network.**

CONTT..

- With the intelligence obtained from a honeypot, security efforts can be **prioritized and focused.**

TYPES OF HONEYPOT

- **Email traps** or spam traps place a **fake email address in a hidden location** where only an automated address harvester will be able to find it.
- Since **the address isn't used for any purpose other than the spam trap,** it's 100% certain that any **mail coming to it is spam.**
- All messages which contain the same content as those sent to the **spam trap can be automatically blocked, and the source IP of the senders can be added to a denylist.**

CONTT..

- A **decoy database** can be set up to **monitor software vulnerabilities** and spot attacks exploiting insecure system architecture or using SQL injection, SQL services exploitation, or privilege abuse.
- A **malware honeypot** mimics software apps and APIs to **invite malware attacks**.
- The characteristics of the malware can then be analyzed to develop anti-malware software or to close vulnerabilities in the API.

CONTT..

- A **spider honeypot** is intended to trap web-crawlers ('spiders') by **creating web pages and links only accessible to crawlers.**
- Detecting crawlers can help you learn how to **block malicious bots**, as well as ad-network crawlers.

By monitoring traffic coming into the honeypot system, you can assess:

- where the cybercriminals are coming from
- the level of threat
- what modus operandi they are using
- what data or applications they are interested in
- how well your security measures are working to stop cyber-attacks

DANGERS OF HONEYPOTS

- If an attacker manages to identify it as a honeypot, they can then proceed to attack your other systems while leaving the honeypot untouched.
- an attacker can create spoofed attacks to distract attention from a real exploit being targeted against your production systems. They can also feed bad information to the honeypot.