INTRUSION DETECTION AND PREVENTION SYSTEM

MODULE 2

TYPES OF IDPS Technologies

Based on the type of events that they monitor and the ways in which they are deployed, divided into four groups:-

1) **Network-Based-** monitors network traffic for particular network segments or devices and analyzes the network to identify suspicious activity

   Deployed at a boundary between networks, such as in proximity to border firewalls or routers, virtual private network (VPN) servers, remote access servers, and wireless networks

2) **Wireless-** monitors wireless network traffic and analyzes its wireless networking protocols to identify suspicious activity. Deployed within range of an organization's wireless network

CONTT…

3) Network Behavior Analysis(NBA)- examines network traffic to identify threats that generate unusual traffic flows, such as **distributed denial of service (DDoS) attacks**, certain forms of **malware (e.g., worms, backdoors), and policy violations**.

Deployed in organization's **internal networks**, and between an organization's networks and **external networks**.

4) Host-Based- monitors the **characteristics of a single host** and the events occurring within that host **for suspicious activity**.

Mainly deployed in publicly **accessible servers** containing confidential information. Notices below characteristics-

a) System logs b) Running processes c) Files access and modification d) System and application configuration changes.

COMPONENETS

The typical components in an IDPS are as follows:

1) **Sensors-** It supply the **initial data about potentially malicious activity.** Sensors monitor and analyze activity. Two types- Network –based or Host-based.
2) **Agents-** Group of processes that run **independently** and are programmed to analyze system behavior or network events to **detect anomalous events and violations of an organization's** security policy.

Advantages- Adaptability, Efficiency, Independence, Scalability, Mobility, etc.

Disadvantages- Resource Allocation, False Alarm, Time, effort and resources needed.

CONTT…

3) Management server- A centralized device that receives information from the sensors or agents and manages them.

Functions-

a) **Data Management**

b) **Alerting**

c) **Event Correlation-** Matching event information from multiple sensors or agents, such as finding events triggered by the same **IP address, is known as correlation.**

d) **High-level Analysis**

e) **Monitoring other components**

f) **Policy Generation and Distribution**

g) **Security Management and Enforcement**

4) Database Server- A repository for event information recorded by sensors, agents, and/or management servers.

5) Console- A program that provides an interface for the IDPS's users and administrators

ARCHITECTURAL MODEL

- An effective architecture is defined as the one in which each machine, device, component, and process performs its role in an effective and **coordinated manner,** resulting in efficient information processing and output, and also appropriate preventive responses that meet the business and operational needs of an organization.

There are three tiered architecture for IDPS-

1) **Single-tiered Architecture- One in which components in an IDS or IPS collect and process data themselves**, rather than passing the output they collect to another set of components. Eg- Host-based intrusion detection tool.

Advantages- Simplicity, low cost, independence from other componenets.

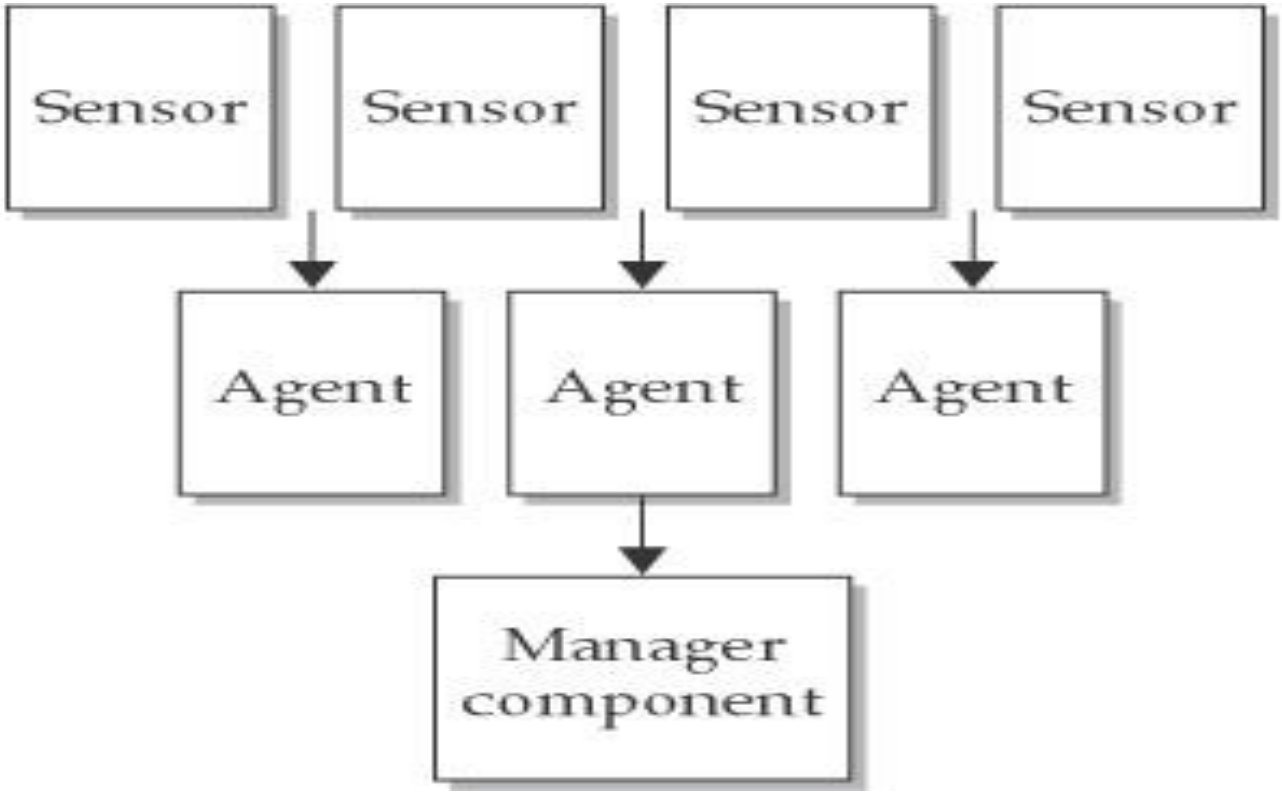
CONTT…

2) Multi- tiered Architecture- A multi-tiered architecture involves **multiple components that pass information to each other**.

Advantages- Greater efficiency and depth of analysis.

3) Peer-to-Peer Architecture- It involves exchanging i**ntrusion-detection and intrusion-prevention information between peer components,** each of which performs the same kinds of functions. Well suited to organizations that have invested enough **to obtain and deploy firewalls capable of cooperating with each other.**

Its simple and major downfall is lack of sophisticated functionality due to the absence of specialized components.



Multi-Tier Architecture

Types of Vulnerability Assessment

Vulnerability **scanning helps** in the **identification of potential security loopholes which can be targeted by hackers** for attacking the computer network system.

Challenges-

- Often requires **input from users which becomes challenging task**.
- Only known vulnerabilities are detected .
- For performing **in-depth scanning assessments**, proper credentials are required for authentication and the unavailability of proper credentials become a hamper.

Divided into two types-

1) Credential based Vulnerability Assessment
2) Non- Credential based Vulnerability Assessment

- **Credential Vulnerability Scan-** Credential-based Vulnerability Assessment Scanning requires credentials **for performing the scanning assessment as well as conducted scanning operation** in **greater depth which provides more accurate results**.

Benefits-

- It performs a **wide variety of scanning operations** compared to the other type of **scanning techniques where credentials are not required** for **validation of user identity**.
- They are well known because of its **accurate results**.
- There is **less load on the computer network** which enhances the **speed and security** of systems in the network.
- Minimizes the **false positive results in scanning**, and the results generated from this scan are known for their **precise results** and **accuracy.**
- **Results generated** from this scan help in **identifying potential risks**, **vulnerabilities, and shortcomings** of the concerned computer network.

CONTT…

Steps to perform:-

1. This scan requires **administrative access** to the systems being scanned and are performed using the same credentials and **privileges as an administrative user**.
2. It performs a thorough **examination of the system**, looking for **vulnerabilities that could be exploited by a malicious attacker.**
3. It can provide a **more accurate representation of a system's security posture,** as they can examine areas of the system that would otherwise be inaccessible to an non-credentialed scan.
4. Credentialed **scans can be performed on both internal and external systems,** making them typically more comprehensive than non-credentialed scans.
5. The results are used to **prioritize remediation efforts**, as the vulnerabilities found are more **likely to be real and exploitable.**

- **Non- Credential Vulnerability Scan-** Non- Credential based Vulnerability Assessment Scanning **do not require credentials for performing the scanning assessment**. Limited scope and less accurate results.

Benefits-

- It can be run on any system, **regardless of whether the scanner has access to the credentials or not.**
- They are quicker and **less resource-intensive.**
- Provide a high level of detail about **the vulnerabilities** present on a system as the scanner **doesn't have to rely on the accuracy of the information provided by the system.**

CONTT…

Steps to perform:-

1. Different from credentialed scans, as they do not require access to the target system's credentials.
2. Rely on **network-level information** and publicly accessible information to **identify vulnerabilities**
3. It involves identifying the **target systems** and **applications** and then probing them for **known vulnerabilities**.
4. Lastly, the scan then generates a **report highlighting any potential security risks and weaknesses.**

- **Credential Scan are ideal in such situation-**

a) When you need a **complete and accurate view** of the vulnerabilities in a system.

b) When you **want to verify that your security measures** are working effectively.

c) Need to **identify and prioritize vulnerabilities** based on their severity and risk level.

- **Non- Credential Scan are ideal in such situation-**

a) When you want a **quick overview of the potential vulnerabilities of a system.**

b) When you **do not have administrative access to the target system.**

c) When you need to **perform a preliminary scan** before conducting a comprehensive credentialed scan.