10. What is an intrusion detection system? Explain its various types with advantages and disadvantages.

Ans:

An Intrusion Detection System (IDS) is a security technology that monitors network or system activities for signs of unauthorized access, security breaches, or malicious activities. It serves as an essential component of cybersecurity infrastructure.

Advantages of IDS in general:

- Early detection of suspicious or malicious activities, allowing for a rapid response to potential threats.
- Helps in identifying patterns and trends in attacks, aiding in the development of more robust security measures.
- Provides valuable forensic data for investigating security incidents.

Disadvantages of IDS in general:

- False positives can occur, where normal activities are flagged as suspicious, leading to unnecessary alerts.
- False negatives are also possible, where actual attacks go undetected.
- Maintenance and tuning can be time-consuming, requiring continuous updates to stay effective against evolving threats.

There main types of Intrusion Detection Systems are :

1. **Network-based Intrusion Detection System (NIDS):**

NIDS monitors network traffic in real-time. It analyzes data packets passing through a network and identifies suspicious or unauthorized activity based on predefined patterns or signatures.

- **Advantages:**

  - Provides visibility into the entire network, making it suitable for detecting attacks across multiple systems.

  - Can identify abnormal patterns or known attack signatures, offering a high level of accuracy.

- **Disadvantages:**

  - May not detect attacks on individual hosts or systems that aren’t directly monitored by the network.

  - Vulnerable to encrypted traffic, as it can’t inspect the contents of encrypted packets.

2. **Host-based Intrusion Detection System (HIDS):**

- **Description:** HIDS is installed on individual hosts (computers or servers) and monitors activities specific to that host, including system logs, file integrity, and application behavior.

- **Advantages:**

  - Provides detailed information about activities on a specific host, making it effective for identifying insider threats or attacks targeting a specific system.

  - Can monitor local activity even if the network is compromised.

- **Disadvantages:**

  - May have a higher false positive rate due to variations in system behavior and configurations.

  - Requires installation and maintenance on each host, which can be

3. Protocol-based Intrusion Detection System (PIDS) is a type of Intrusion Detection System (IDS) that focuses on monitoring network traffic for deviations from established protocol standards. It looks for anomalies or violations in the way network protocols are used, which can indicate potential security threats.

Advantages of Protocol-based Intrusion Detection System (PIDS):

- **Early Detection:** It can identify suspicious behavior or deviations from standard protocols, allowing for early detection of potential threats.

- **Protocol-specific Analysis:** PIDS is specialized in analyzing specific network protocols, providing a focused approach to identifying anomalies.

Disadvantages of Protocol-based Intrusion Detection System (PIDS):

- **Limited Scope:** PIDS primarily focuses on monitoring protocol compliance, which may not detect more sophisticated or non-standard attacks.

- **False Positives:** It may generate false alarms if legitimate traffic exhibits unusual behavior due to network changes or configurations.

- **Dependent on Protocol Knowledge:** PIDS requires a deep understanding of specific protocols, making it less suitable for organizations with diverse or complex network environments.

4. Application Protocol-based Intrusion Detection System (APIDS) monitors network traffic to detect anomalies in application-layer protocols. It focuses on identifying suspicious behavior within specific applications, enhancing security at a more granular level.

Advantages:

- Targets application-layer vulnerabilities

- Offers detailed insights into application-specific threats

Disadvantage:

- Limited to application-layer monitoring, potentially missing lower-level or non-application-specific attacks.