Written Assignment 2

Q. What is Intrusion Detection System? Explain different types of intrusion detection systems with their working. State the advantages and limitations of each.

→ An Intrusion Detection System (IDS) is a security technology that monitors and analyzes network traffic or system activities for signs of unauthorized access, malicious activities, or policy violations. IDSs are crucial components of a comprehensive cybersecurity strategy and help organizations detect and respond to security incidents in real-time. There are two primary types of Intrusion Detection Systems: Network-based IDS (NIDS) and Host-based IDS (HIDS), each with its working principles, advantages, and limitations.

1. Network-Based Intrusion Detection System (NIDS):

- **Working:** NIDS monitors network traffic, including packets and data flows, to identify suspicious or malicious activities. It uses various detection techniques, such as signature-based detection (looking for known attack patterns) and anomaly-based detection (identifying deviations from normal network behavior).

- **Advantages:**

  - **Comprehensive Coverage:** NIDS can monitor network traffic across multiple hosts and devices, providing a holistic view of network activity.

  - **Real-time Detection:** It can detect suspicious activities as they occur, allowing for immediate response.

  - **Scalability:** NIDS can be deployed at critical network points to protect a large network infrastructure.

- **Limitations:**

  - **Limited Visibility:** NIDS cannot detect attacks that occur exclusively on a single host, such as insider threats or attacks within encrypted traffic.

  - **False Positives:** NIDS may generate false alarms if it misinterprets legitimate traffic as malicious.

  - **Encrypted Traffic:** It struggles to inspect encrypted traffic without decryption, which can introduce privacy and legal concerns.

2. Host-Based Intrusion Detection System (HIDS):

- **Working:** HIDS is installed on individual hosts (servers, workstations, etc.) and monitors activities within the host's operating system and applications. It looks for unusual behavior or signs of compromise, such as changes to system files, unauthorized access, or suspicious processes.

- **Advantages:**

  - **In-depth Visibility:** HIDS can detect attacks and vulnerabilities specific to the host, including insider threats.

  - **Minimal Network Impact:** It doesn't rely on network traffic monitoring and is effective even in isolated environments.

  - **Granular Control:** Provides detailed information about host-specific activities.

- **Limitations:**

  - **Limited Network Visibility:** HIDS cannot detect network-level attacks that don't involve the host being monitored.

  - **Installation and Maintenance:** Deploying and managing HIDS on a large number of hosts can be resource-intensive.

  - **False Positives:** Like NIDS, HIDS can generate false alarms if it misinterprets normal activities as malicious.

3. Hybrid Intrusion Detection System:

- **Working:** Hybrid IDS combines both NIDS and HIDS components to provide a more comprehensive approach to intrusion detection. It leverages the strengths of both types to improve accuracy and coverage.

- **Advantages:**

  - **Enhanced Detection:** Hybrid IDS can detect threats at both network and host levels, increasing the chances of identifying sophisticated attacks.

  - **Improved Context:** It provides a more comprehensive view of an incident by correlating network and host data.

  - **Better Scalability:** It can adapt to various network architectures and security requirements.

- **Limitations:**

- **Complexity:** Hybrid IDS can be more complex to deploy and manage compared to standalone NIDS or HIDS.

- **Resource Intensive:** It may require additional resources to support both network and host-based monitoring.