Animesh Parab 88 T2---T21

Assignment 2

An Intrusion Detection System (IDS) is a security technology used to monitor network or system activities for suspicious or malicious behavior and to identify potential security threats. IDSs are crucial for maintaining the integrity and security of computer networks and systems. There are several types of IDSs, each with its own approach to detecting intrusions. Below, I'll explain the different types of IDSs and their working, along with their advantages and limitations:

Signature-Based IDS (Network-Based and Host-Based):

- **Definition:** Signature-based IDSs rely on predefined patterns or signatures to identify known threats or attacks.
- **Working:**
- **Network-Based Signature IDS:** It inspects network traffic, such as packets and network flows, searching for patterns that match known attack signatures. For example, if the IDS identifies a packet with a signature matching a known virus, it raises an alert.
- **Host-Based Signature IDS:** This type monitors activities on individual hosts or endpoints, such as servers or workstations. It reviews system logs, file changes, and processes to detect known malicious patterns.
- **Advantages:**
- Effective at detecting well-known threats.
- Low false positive rates as it's looking for specific patterns.
- Efficient in terms of resource usage.
- **Limitations:**
- Ineffective against zero-day attacks because they lack known signatures.
- Regular signature updates are necessary to remain effective.
- Limited to identifying threats based on established patterns.
- **Example:** A network-based signature IDS might identify and alert the IT team to a known pattern of SQL injection attempts in incoming web traffic.

2. **Anomaly-Based IDS (Network-Based and Host-Based):**

- **Definition:** Anomaly-based IDSs establish a baseline of normal behavior and then flag any deviations from this baseline as potential intrusions.
- **Working:**
- **Network-Based Anomaly IDS:** It learns the typical patterns of network traffic and raises alerts when it detects significant deviations from the norm, such as unusual data volume or unusual port usage.
- **Host-Based Anomaly IDS:** This type observes the behavior of individual systems or users. It tracks file access, login times, and system processes, and alarms if any behavior significantly deviates from what's typical.

- **Advantages:**
- Can detect zero-day attacks and previously unseen threats.
- Adapts to changing attack patterns.
- Effective against insider threats as it can detect unusual internal behavior.
- **Limitations:**
- Higher false positive rates, as any deviation from the baseline may trigger alerts.
- Requires substantial historical data to establish accurate baselines.
- Might not catch sophisticated attacks that mimic normal behavior well.
- **Example:** A host-based anomaly IDS could raise an alert when a user, who typically logs in at 9 AM and logs out at 6 PM, suddenly starts accessing the system at midnight.

3. **Hybrid IDS:**
   - **Definition:** Hybrid IDS combines elements of signature-based and anomalybased detection to enhance overall threat detection capabilities.
   - **Working:** Hybrid IDS simultaneously employs both signature-based and anomaly-based techniques. It looks for known attack patterns and deviations from normal behavior.
   - **Advantages:**
   - Balances the strengths of signature-based and anomaly-based IDS.
   - Offers a more comprehensive security posture.
   - **Limitations:**
   - It can be resource-intensive due to running both types of analysis.
   - Still vulnerable to false positives and false negatives, albeit potentially to a lesser extent.
   - **Example:** A hybrid IDS might detect a known malware signature in an incoming packet and also raise an alert if that packet contains unusual or unexpected data patterns.

4. **Behavior-Based IDS:**
   - **Definition:** Behavior-based IDS focuses on the behavior of software applications and processes to identify deviations from expected behavior.
   - **Working:** It builds profiles of how applications and processes should behave. When it detects significant changes or actions inconsistent with the established profiles, it triggers an alert.
   - **Advantages:**
   - Effective against advanced persistent threats (APTs) and other complex attacks.
   - Less reliant on specific attack signatures.
   - **Limitations:**
   - Requires significant computational resources to profile and analyze behavior.
   - May generate false positives when legitimate software behavior changes.

- **Example:** A behavior-based IDS might alert administrators when a web server, which typically only handles incoming requests, suddenly initiates unauthorized outbound network connections, indicating a potential breach.

Each type of IDS has its place in a comprehensive security strategy. Organizations often use a combination of these IDS types to maximize threat detection while minimizing false alarms and vulnerabilities.