IAS2 Reviewer

INTRUSION DETECTION AND PREVENTION SYSTEMS

Intrusion– An adverse event in which an attacker attempts to enter an information system or disrupts its normal operations, almost always with the intent to do harm.

Intrusion Detection – consists of procedures and systems that identify system intrusions.

Intrusion Reaction – encompasses the actions an organization takes when an intrusion is detected.

Intrusion Correction – activities that completes the restoration of operations to a normal state and seek to identify the source and method of the intrusion.

Intrusion Detection System – A system capable of automatically detecting an intrusion into an organization's networks or host systems.

Intrusion Detection and Prevention Systems – The general term for a system that can both detect and modify its configuration and environment to prevent intrusions.

IDPSs use several techniques, which can be divided into the following groups:

- Terminating the user session or network connection over which the attack is being conducted.
- Blocking access to the target system or systems from the source of the attack, such as a compromised user account, inbound IP address, or other attack characteristic.
- Blocking all access to the targeted information asset.

IDPS can dynamically modify its environment by changing the configuration of other security controls to disrupt an attack.

Some IDPSs are capable of changing an attack's components by replacing malicious content with benign material or by quarantining a network packet's contents.

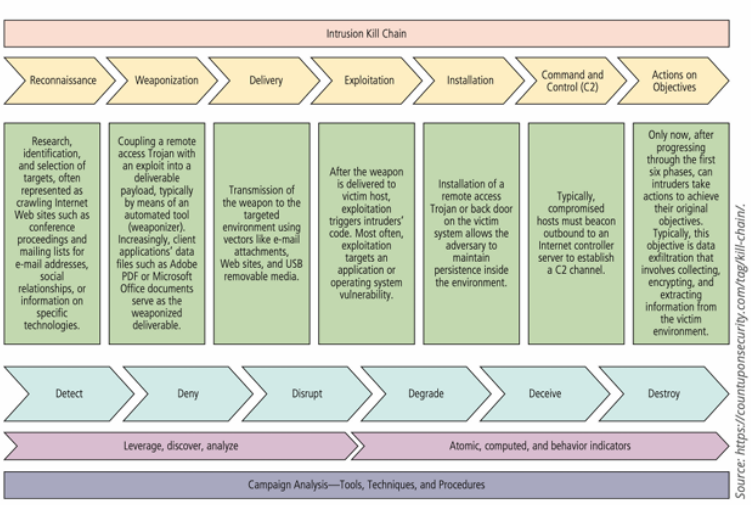
IDPS TERMINOLOGIES

1. **Alarm or alert:** An indication or notification of a system that's been attacked or under attack.
2. **Alarm clustering and compaction**: A process of grouping almost identical alarms.
3. **Alarm filtering**: The process of classifying IDPS alerts.
4. **Confidence value**: The measure of an IDPS's ability to correctly detect and identify certain types of attacks.
5. **Evasion:** The process by which attackers change the format or timing of their attack.
6. **False Attack Stimulus**: An event that triggers an alarm when no actual attack is in progress.
7. **False Negative**: The failure of a technical control to react to an actual attack event.
8. **False Positive**: An alert or alarm that occurs in the absence of an actual attack.
9. **Noise**: In incident response, alarm events that are accurate and noteworthy but do not pose significant threats to information security.
10. **Site Policy**: The rules and configuration guidelines governing the implementation and operation of IDPSs within the organization.
11. **Site Policy Awareness**: An IDPS's ability to dynamically modify its configuration in response to environmental activity.

12. **True Attack Simulus**: An event that triggers an alarm and causes in IDPS to react as if a real attack is in progress.
13. **Tuning**: The process of adjusting an IDPS to maximize its efficiency in detecting true positives while minimizing false positives and false negatives.

WHY USE AN IDPS

- To log data for later analysis
- To serve as a deterrent by increasing the fear of detection among would-be attackers.
- To provide a level of quality control for security policy implementation.



Cyberattack Kill Chain

TYPES OF IDPSS

1. Network-based IDPS – An IDPS that resides on a computer or appliance connected to a segment of an organization's network and monitors traffic on that segment, looking for indication of ongoing or successful attacks.
    a. Sensor or Agent: A hardware and software component deployed on a remote computer or network segment and designed to monitor network or system traffic for suspicious activities and report back to the host application.
        i. Monitoring Port: specially configured connection on a network device that can view all the traffic that moves through the device; also known as a switched port analysis port or mirror port.
    - To determine whether an attack has occurred or is under way, NIDPSs compare measured activity to known signatures in their knowledge base.
    - The comparisons are made through a special implementation of the TCP/IP stack that that reassembles the packets and applies protocol stack verification, application protocol verification, other verification and comparison techniques.
2. **Protocol Stack Verification**: The process of examining and verifying network traffic for invalid data packets – that is, packets that are malformed under the rules of the TCP/IP protocol.
3. **Application Protocol Verification**: The process of examining and verifying the higher-order protocols (HTTP, FTP, and Telnet) in network traffic for unexpected packet behavior or improper use.
4. It may be necessary to have more than one NIDPS installed, with one of them performing protocol stack verification and one performing protocol stack

verification and one performing application protocol verification.

ADVANTAGES OF NIDPS

- Good network design and placement of NIDPS devices can enable an organization to monitor a large network using only a few devices.
- NIDPSs are usually passive devices and can be deployed into existing networks with little or no disruption to normal network operations.
- NIDPSs are not usually susceptible to direct attack and may not be detectable by attackers.

DISADVANTAGES OF NIDPS

- An NIDPS can become overwhelmed by network volume.
- NIDPSs require access to all traffic to be monitored.
- NIDPSs cannot analyze encrypted packets.
- NIDPSs cannot reliably ascertain whether an attack was successful.
- Some forms of attack are not easily discerned by NIDPSs.

TYPES OF IDPSS

- Wireless IDPS – A wireless IDPS monitors and analyzes wireless network traffic, looking for potential problems with the wireless protocols (Layers 2 and 3 of the OSI model).
- The implementation of wireless IDPSs includes the following issues:
    - Physical Security
    - Sensor Range
    - Access Point and Wireless Switch Locations
    - Wired Network Connections
    - Cost
- Network Behavior Analysis System: Identify problems related to the flow of network traffic.
- Intrusion Detection and Prevention typically includes the following relevant flow data:
    - Source and destination IP addresses
    - Source and destination TCP or UDP ports or ICP types and codes.
    - Number of packets and bytes transmitted in the session
    - Starting and ending timestamps for the session.
    - Most NBA sensors can be deployed in passive mode only, using the same connection methods.
        - Detects DoS attacks
        - Detects scanning
        - Detects worms
        - Detects unexpected application services.
        - Detects policy violations
    - Inline sensors are typically intended for network perimeter use, so they would be deployed in close proximity to the perimeter firewalls.
- **Host-based:** an IDPS that resides on a particular computer or server,

known as the host, and monitor activity only on that system.

ADVANTAGES OF HIDPSs

- It can detect local events on host systems and attacks that may elude a network-based IDPS.
- Encrypted traffic will be decrypted and is available for processing.
- It can detect inconsistencies using the records in the audit logs.

DISADVANTAGES OF HIDPSs

- Pose more management issues
- Vulnerable both to direct attacks and against the host operating system.
- Susceptible to some DoS attacks
- Uses large amounts of disk space
- Inflict a performance overhead.

IDPS DETECTION METHODS

Signature-based Detection: the examination of system or network data in search of patterns that match known attack signatures.

Signature-based technology is widely used because many attacks have clear and distinct signatures

Anomaly-based Detection: Compares current data and traffic patterns to an established baseline of normalcy. It sends an alert when exceeding the clipping level.

- Clipping Level: A predefined assessment level that triggers a predetermined response when surpassed.

Stateful Protocol Analysis: Comparison of vendor-supplied profiles of protocol use and behavior against observed data and network patters to detect misuse and attacks.

Log File Monitor – An attack detection method that review log files generated by computer system looking for patterns and signatures.

Security Information and Event Management – Specifically tasked to collect and correlate events and other log data from a number of servers or devices for the purpose of filtering, correlating, analyzing, storing, reporting, and acting.

- Supports threat detection and informs many aspects of threat intelligence.
    - Threat Intelligence – A process used to develop knowledge to understand the actions and intentions of threat actors.

Larger Organizations are faced with several needs that SIEM platforms can address:
1. Aggregation

2. Correlation

3. Integration

4. Detection

5. Enablement

6. Tracking

7. Possible Detection

Essential Capabilities of an Analytics-Driven SIEM System should provide the following:

1. Real-time Monitoring
2. Incident Response
3. User Monitoring
4. Threat Intelligence
5. Analytics and Threat Detection

IDPS RESPONSE BEHAVIOR

- The system administrator must ensure that a response to an attack or potential attack not

inadvertently exacerbate the situation.

- IDPS responses can be classified as active or passive.
    - **Active** – definitive action that is automatically initiated.
    - **Passive** – simply report the information they have collected.

These can be configured for the responses of an IDPS:

1. Audible/Visual Alarm
2. SNMP Traps and Plugins
3. E-mail Message
4. Phone or SMS Message

The following list describes some of the responses:

1. Log Entry
2. Evidentiary Packet Dump
3. Acting against the intruder.
4. Launching a program
5. Reconfiguring a firewall
6. Terminating the Session
7. Terminating the connection

STRENGTHS OF IDPSS

- Monitoring and analysis.
- Testing
- Baselining
- Recognizing patterns of system
- Recognizing patterns of activity
- Managing Operating System Audit and Logging Mechanisms
- Alerting
- Measuring
- Providing default security information
- Allowing people to perform important security monitoring functions

LIMITATION OF IDPSS

1. Compensating
2. Instantaneously detecting, reporting, and responding to an attack
3. Detecting newly published attacks or variants of existing attacks
4. Effectively responding to attacks launched by sophisticated attackers
5. Automatically investigating attacks without human intervention.
6. Resisting all attacks
7. Compensating for problems
8. Dealing effectively with switched networks

DEPLOYMENT AND IMPLEMENTATION OF AN IDPS

NIST SP 800-94, Rev. 1, provides the following recommendations or implementation:

- Organizations should ensure that al IDPS components are appropriately, as IDPS are a prime target for attackers.
- Organizations should consider using multiple types of IDPS technologies to achieve more comprehensive and accurate detection and prevention of malicious activity.
- Organizations that plan to use multiple types of IDPS technologies or multiple products of the same IDPS technology type should consider whether the IDPSs should be integrated.
- Before evaluating IDPS products, organizations should define the requirements that the products should meet.
- When evaluating IDPS products, organizations should consider using combination of data sources

to evaluate the products characteristics and capabilities.

IDPS CONTROL STRATEGIES

- **Control Strategy:** Determines how an organization supervises and maintains the configurations of an IDPS.
- 3 Common control strategies are **Centralized, Partially Distributed, and Fully Distributed.**

Centralized – All control functions are managed in a central location

Fully Distributed – All control functions are applied at the physical location of each IDPS component

IDPS DEPLOYMENT

An organization selects an IDPS and prepares for implementation, planners must select a deployment strategy that is based on a careful analysis of the organization's information security requirements and that integrates with the existing IT infrastructure while causing minimal impact.

DEPLOYING HOST-BASED IDPSS

- Deployment begins on the most critical systems first.
- Practice an implementation on a test server.
- Installation continues until all systems are installed.
- Provide ease of management, control, and reporting.

MEASURING THE EFFECTIVENESS OF IDPSS

1. Threshold – Value that sets the limit between normal and abnormal behavior.
2. Blacklists – Addresses that a system has been associated with malicious activity.
3. Whitelists – Systems are known to be benign.
4. Alert Settings
5. Code Viewing and Editing