Intrusion Detection System (IDS): Types, Techniques, and Applications

Intrusion detection systems (IDS) are designed to identify suspicious and malicious activity through network traffic. It enables real-time intrusion detection on your network to help optimize intrusion detection. So, let's get to know the meaning of an intrusion detection system and how it works. and how it works.

What Is an Intrusion Detection System?

An intrusion detection system definition includes installing a monitoring system that helps detect suspicious activities and issue alerts about them. Depending upon these alerts, a SOC (security operations center) analyst or the incident responder investigates the issue and takes the required steps to eradicate the threat.

While these systems are quite effective for detecting malicious activity, they sometimes generate false alarms. So, organizations need to fine-tune them at the time of installation. This means you need to properly set up the intrusion detection system to identify what normal traffic on the network looks like.

Additionally, the intrusion prevention system also keeps a check on the network packets to detect malicious activity.

Why Are Intrusion Detection Systems Important?

The goal of IDS is to monitor the network assets to detect inappropriate behavior in the network. Attackers continuously develop new exploits and affect techniques that are designed to affect the defense. Some attacks are for obtaining user credentials that grant access to the network and data. A Network Intrusion detection system (NIDS) is important for network security as it allows you to respond to malicious traffic.

An intrusion detection system's prime benefit is ensuring that the respective person is notified when the attack happens. In addition, a network intrusion detection system keeps a check on both inbound and outbound traffic on the network and monitors data traversing between the system and the network.

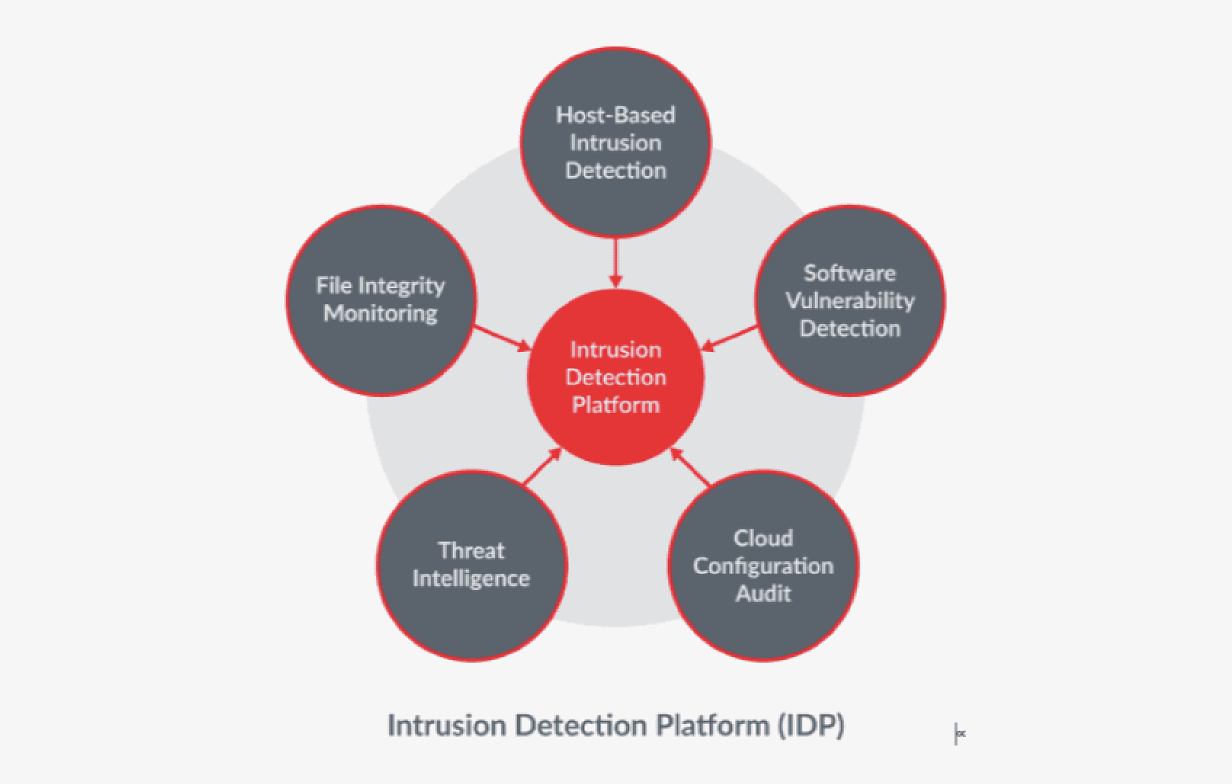
How Do Intrusion Detection Systems Work?

IDS operates through a process where different events on the network are analyzed and monitored to detect incidents of malicious activity or any kind of security violation. It is placed out from the real-time communication band in your network to work as a detection system. It uses SPAN or TAP port to analyze the copy of inline network packets to ensure that the traffic coming is not malicious.

So, if you set an IDS program, the system will be able to:

- Recognize attack patterns from the network packets
- Monitor the user behavior
- Identify the abnormal traffic activity
- Ensure that user and system activity do not go against security policies

Types of an Intrusion Detection System


Host-Based Intrusion Detection
File Integrity Monitoring
Software Vulnerability Detection
Intrusion Detection Platform
Threat Intelligence
Cloud Configuration Audit
Intrusion Detection Platform (IDP)

There are many different types of IDS for protecting computer networks. Below are popular types of intrusion detection systems:

1. Host Intrusion Detection Systems (HIDS):

HIDS host-based intrusion detection system runs on independent devices, i.e., a host on the network monitors the incoming and outgoing packets and alerts the administrator about malicious activity. It takes a snapshot of the existing system files to identify the abnormalities. If there are any discrepancies among the file sent or if anything got deleted, an alert is sent to the administrator for further investigations.

2. Protocol-Based Intrusion Detection System (PIDS):

PIDS, a Protocol-based Intrusion Detection System, is a system or agent that resides consistently at the front end of the server to control and interpret the protocol between the user and the server. PIDS is for securing the web server by monitoring the HTTPS protocol stream. A typical use of PIDS is at the front end of the web server, keeping a check on the HTTP or HTTPS stream.

3. Application Protocol-Based Intrusion Detection System (APIDS):

An application-based intrusion detection system is a system that stays within a group of servers. It identifies the intrusions by monitoring and interpreting the communication on application-specific protocols.

APIDS uses machine language to establish the baseline of the expected system behavior in terms of bandwidth, parts, protocol, and device usage.

4. Hybrid Intrusion Detection System:

A hybrid intrusion detection system results from two or more approaches to the intrusion detection system. in this, the host agent or the system data is combined with the network information to develop a complete view of network systems. This system is quite effective in comparison to other IDS.

Detection Method of IDS Deployment

Any IDS uses different methods for detecting malicious network traffic. Some of them are:

1. Signature Detection:

Signature-based intrusion detection systems use fingerprints of known threats to keep a check on them. Once the malicious traffic or packets are detected, the IDS generates a signature to scan the incoming traffic to detect known malicious patterns. The signature-based IDS can detect the attacks whose patterns are already present in the system but are unable to detect new or unknown malicious or attack network traffic.

2. Anomaly Detection:

The anomaly-based intrusion detection system was introduced to detect unknown malicious attacks as new attack methods are developed quickly. This detection method uses machine learning to create a trustful activity model, and anything that comes is compared with that model to detect malicious traffic or patterns. The machine learning-based method has better-generalized property as compared to the signature-based IDS and are trained with the intrusion detection system application and hardware configurations.

3. Hybrid Detection:

This IDS uses both signature-based as well as anomaly-based detection system and enable it to detect potential threats with a minimum error rate.

Benefits of Intrusion Detection Systems

Apart from raising the alarms, the intrusion detection system software also helps in configuring rules, policies, and respective actions to be taken.

Below are the benefits of using an IDS:

1. It keeps a check on the routers, firewalls, key servers, and files and uses its database to raise the alarm and send notifications.
2. Offer centralized management for the correlation of the attack.
3. Act as an additional layer of protection for the company.
4. It analyzes different attacks, identifies their patterns, and helps the administrator to organize and implement effective control.
5. Provide system administrators the ability to quantify the attack.
6. An intrusion detection system in cyber security help detects cybersecurity problems.

Challenges of Intrusion Detection Systems

There are four key challenges that businesses face when managing IDS systems:

1. Ensuring Effective Deployment:

To ensure a high level of visibility, companies must ensure that their wireless intrusion detection system is optimized and installed correctly. While deploying IDS can be tricky, and if not done properly, it may create vulnerabilities for critical assets.

2. Understanding and Investigating Alerts:

IDS alerts give very little information, which, sometimes, is hard to investigate. You may lag with information like what caused the attack or what further actions are required to oppose a threat. Also, investigating the IDS alerts can be time and resource-intensive, which may require additional information to identify the seriousness of the attack.

3. Managing a High Volume Of Alerts:

Since there is the vast majority of attacks are generated by intrusion detection, it may put the burden on internal teams to identify each one of them. Sometimes, these system alerts are false positives, which are hard to screen. Also, some IDS come pre-loaded with some defined alert signatures that are insufficient for many organizations.

4. Knowing How To Tackle Threats:

A common issue that organizations face is the lack of appropriate incident response capability. Identifying a problem is half a thing; knowing how to respond appropriately is a challenging and critical thing. An effective incident response needs an expert who knows how to remediate threats and what procedures are required to address the issue. Sometimes a home intrusion detection system gives false alarms, so keep a check on the type of threats and how you need to handle them. The cyber security team needs to be updated with the latest progress and update in IDS and key domains of cyber security. Courses such as **CEH training** are very useful for keeping pace with learning.

IDS Vs. Firewall

Installing an intrusion Detection System project and a firewall offers cybersecurity solutions deployed to protect the network or its endpoint.

An IDS is a passive monitoring device that helps detect threats and generate alerts. It enables SOC (security operation center) analysts or incident responders to detect and respond to the threat. An IDS provides no protection to the endpoint.

On the other hand, a firewall is an active protective device and is more like an Intrusion Prevention System (IPS). It performs analysis of the metadata of the network packets and helps block/allow the traffic based on some pre-set rules. This creates a boundary on which some types of traffic or protocols cannot pass.

An IPS is more like an IDS, but the only difference is that it blocks the identified threats instead of raising the alert. This functionality makes IPS more popular among firewalls, and many next-gen firewalls are integrating this functionality.

How to Select An IDS Solution

Once you know what IDS is and its detection, you need to follow these steps to select an IDS solution:

1. Identify The Baseline: To ensure that your IDS works appropriately, set a baseline so you would know what's coming on your network. Keep in mind that every network carries additional traffic, and defining a pre-set initial baseline help prevent false negatives. An intrusion detection system in network security will keep your network protected from firewalls. To ensure that your IDS works appropriately, set up a baseline so that you would know what's coming on your network. Keep in mind that every network carries different traffic, and defining a pre-set initial baseline help prevent false negatives. An intrusion detection system in network security will keep your network protected from firewalls.

2. Define The Deployment: Always deploy the distributed intrusion detection system at the highest point to not overwhelm the system with data. Place it at the edge, behind the firewall, or install multiple IDSes if you are dealing with a lot of traffic.

3. Test The IDS: Test the system to ensure it detects the potential threats and responds to them properly. Use test datasets or have security professionals do a pen test.

Conclusion:

Keeping in mind the challenges of ongoing system monitoring, maintenance, and alert investigation, many organizations wish to consider having secure network-based intrusion detection systems. A managed IDS service avoids recruiting a dedicated security person and sometimes includes the requisite technology, minimizing the need to maintain capital expenditure.