What is an IDS?

Compiled by - Asst. Prof. Sridhar Iyer

An intrusion detection system (IDS) is a software application or hardware appliance that monitors traffic moving on networks and through systems to search for suspicious activity and known threats, sending up alerts when it finds such items.

The overall purpose of an IDS is to inform IT personnel that a network intrusion may be taking place. Alerting information will generally include information about the source address of the intrusion, the target/victim address, and type of attack that is suspected.

Each IDS is programmed to analyze traffic and identify patterns in that traffic that may indicate a cyber attack of various sorts. An IDS can identify “traffic that could be considered universally malicious or noteworthy,”

How do intrusion detection systems work?

Intrusion detection systems are used to detect anomalies with the aim of catching hackers before they do real damage to a network. They can be either network- or host-based. A host-based intrusion detection system is installed on the client computer, while a network-based intrusion detection system resides on the network.

Intrusion detection systems work by either looking for signatures of known attacks or deviations from normal activity. These deviations or anomalies are pushed up the stack and examined at the protocol and application layer. They can effectively detect events such as Christmas tree scans and domain name system (DNS) poisonings.

An IDS may be implemented as a software application running on customer hardware or as a network security appliance. Cloud-based intrusion detection systems are also available to protect data and systems in cloud deployments.

An IDS can be contrasted with an intrusion prevention system (IPS), which monitors network packets for potentially damaging network traffic, like an IDS, but has the primary goal of preventing threats once detected, as opposed to primarily detecting and recording threats.

IDS vs. IPS

Most organizations have either an IDS or an IPS, and many have both as part of their security information and event management framework.

	IDS	IPS
NAME	Intrusion detection system	Intrusion prevention system
DESCRIPTION	A system that monitors network traffic for suspicious activity and alerts users when such activity is discovered.	A system that monitors network traffic and alerts for suspicious activity, like an IDS, but also takes preventative action against suspicious activity.
LOCATION	A host-based intrusion detection system is installed on the client computer. A network-based intrusion detection system resides on the network.	Located between a company's firewall and the rest of its network.
USE	Warns of suspicious activity taking place, but it doesn't prevent it.	Warns of suspicious activity taking place and prevents it.
FALSE POSITIVE	IDS false positives are usually just a minor inconvenience. Although the IDS incorrectly labels legitimate traffic as malicious, it does not prevent the traffic from entering the network.	IPS false positives can be more serious. When an IPS mistakes legitimate traffic for a threat, it stops the legitimate traffic from entering the network, which could impact any part of the organization, not just the IT team.

Different types of intrusion detection systems

IDSes come in different flavors and detect suspicious activities using different methods, including the following:

1. A **network intrusion detection system (NIDS**) is deployed at a strategic point or points within the network, where it can monitor inbound and outbound traffic to and from all the devices on the network.

2. A **host intrusion detection system (HIDS)** runs on all computers or devices in the network with direct access to both the internet and the enterprise's internal network. A HIDS has an advantage over a NIDS in that it may be able to detect anomalous network packets that originate from inside the organization or malicious traffic that a NIDS has failed to detect. A HIDS may also be able to identify malicious traffic that originates from the host itself, such as when the host has been infected with malware and is attempting to spread to other systems.

3. A **signature-based intrusion detection system (SIDS)** monitors all the packets traversing the network and compares them against a database of attack signatures or attributes of known malicious threats, much like antivirus software.

4. An **anomaly-based intrusion detection system (AIDS)** monitors network traffic and compares it against an established baseline to determine what is considered normal for the network with respect to bandwidth, protocols, ports and other devices. This type often uses machine learning to establish a baseline and accompanying security policy. It then alerts IT teams to suspicious activity and policy violations. By detecting threats using a broad model instead of specific signatures and attributes, the anomaly-based detection method improves upon the limitations of signature-based methods, especially in the detection of novel threats.

Historically, intrusion detection systems were categorized as passive or active. A passive IDS that detected malicious activity would generate alert or log entries but would not take action; an active IDS, sometimes called an intrusion detection and prevention system (IDPS), would generate alerts and log entries but could also be configured to take actions, like blocking IP addresses or shutting down access to restricted resources.

Capabilities of intrusion detection systems:

Intrusion detection systems monitor network traffic in order to detect when an attack is being carried out by unauthorized entities. IDSes do this by providing some -- or all -- of these functions to security professionals:

1. Monitoring the operation of routers, firewalls, key management servers and files that are needed by other security controls aimed at detecting, preventing or recovering from cyberattacks.

2. Providing administrators a way to tune, organize and understand relevant OS audit trails and other logs that are otherwise difficult to track or parse.

3. providing a user-friendly interface so non expert staff members can assist with managing system security.

4. Including an extensive attack signature database against which information from the system can be matched.

5. Recognizing and reporting when the IDS detects that data files have been altered;
generating an alarm and notifying that security has been breached; and
reacting to intruders by blocking them or blocking the server.

Benefits of intrusion detection systems

Intrusion detection systems offer organizations several benefits, starting with the ability to identify security incidents. An IDS can be used to help analyze the quantity and types of attacks; organizations can use this information to change their security systems or implement more effective controls.

An intrusion detection system can also help companies identify bugs or problems with their network device configurations. These metrics can then be used to assess future risks.

Intrusion detection systems can also help the enterprise attain regulatory compliance. An IDS gives companies greater visibility across their networks, making it easier to meet security regulations. Additionally, businesses can use their IDS logs as part of the documentation to show they are meeting certain compliance requirements.

Intrusion detection systems can also improve security responses. Since IDS sensors can detect network hosts and devices, they can also be used to inspect data within the network packets, as well as identify the OSes of services being used.

Using an IDS to collect this information can be much more efficient than manual censuses of connected systems.

Challenges of intrusion detection systems

IDSes are prone to false alarms -- or false positives. Consequently, organizations need to fine-tune their IDS products when they first install them. This includes properly configuring their intrusion detection systems to recognize what normal traffic on their network looks like compared to potentially malicious activity.

However, despite the inefficiencies they cause, false positives don't usually cause serious damage to the actual network and simply lead to configuration improvements. A much more serious IDS mistake is a **false negative**, which is when the IDS misses a threat and mistakes it for legitimate traffic. In a false negative scenario, IT teams have no indication that an attack is taking place and often don't discover until after the network has been affected in some way.

It is better for an IDS to be oversensitive to abnormal behaviors and generate false positives than it is to be undersensitive, generating false negatives.

False negatives are becoming a bigger issue for IDSes -- especially SIDSes -- since malware is evolving and becoming more sophisticated. It's becoming harder to detect a suspected intrusion because new malware may not display the previously detected patterns of suspicious behavior that IDSes are typically designed to detect. As a result, there is an increasing need for IDSes to detect new behavior and proactively identify novel threats and their evasion techniques as soon as possible.