Intrusion Detection System (IDS)

An **Intrusion Detection System (IDS)** is a system that monitors **network traffic** for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms.

Although intrusion detection systems monitor networks for potentially malicious activity, they are also disposed to false alarms. Hence, organizations need to fine-tune their IDS products when they first install them. It means properly setting up the intrusion detection systems to recognize what normal traffic on the network looks like as compared to malicious activity.

Intrusion prevention systems also monitor network packets inbound the system to check the malicious activities involved in it and at once sends the warning notifications.

Classification of Intrusion Detection System:

IDS are classified into 5 types:

1. **Network Intrusion Detection System (NIDS):**

   Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator. An example of an NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying crack the firewall.

2. **Host Intrusion Detection System (HIDS):**

   Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission critical machines, which are not expected to change their layout.

3.**Protocol-based Intrusion Detection System (PIDS):**

Protocol-based intrusion detection system (PIDS) comprises of a system or agent that would consistently resides at the front end of a server, controlling and interpreting the protocol between a user/device and the server. It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accept the related HTTP protocol. As HTTPS is un-encrypted and before instantly entering its web presentation layer then this system would need to reside in this interface, between to use the HTTPS.

4.**Application Protocol-based Intrusion Detection System (APIDS):**

Application Protocol-based Intrusion Detection System (APIDS) is a system or agent that generally resides within a group of servers. It identifies the intrusions by monitoring and interpreting the communication on application specific protocols. For example, this would monitor the SQL protocol explicit to the middleware as it transacts with the database in the web server.

5. **Hybrid Intrusion Detection System :**

Hybrid intrusion detection system is made by the combination of two or more approaches of the intrusion detection system. In the hybrid intrusion detection system, host agent or system data is combined with network information to develop a complete view of the network system. Hybrid intrusion detection system is more effective in comparison to the other intrusion detection system. Prelude is an example of Hybrid IDS.

Detection Method of IDS:

1. **Signature-based Method:**

Signature-based IDS detects the attacks on the basis of the specific patterns such as number of bytes or number of 1's or number of 0's in the network traffic. It also detects on the basis of the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures.

Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in system but it is quite difficult to detect the new malware attacks as their pattern (signature) is not known.

2.

3.Anomaly-based Method:

Anomaly-based IDS was introduced to detect the unknown malware attacks as new malware are developed rapidly. In anomaly-based IDS there is use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in model. Machine learning based method has a better generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.

Comparison of IDS with Firewalls:

IDS and firewall both are related to the network security but an IDS differs from a firewall as a firewall looks outwardly for intrusions in order to stop them from happening. Firewalls restrict access between networks to prevent intrusion and if an attack is from inside the network it don’t signal. An IDS describes a suspected intrusion once it has happened and then signals an alarm.

What is the function of an intrusion detection system on a network?

Intrusion detection is a passive technology; it detects and acknowledges a problem but interrupt the flow of network traffic, Novak said. "As mentioned, the purpose is to find and alert on noteworthy traffic. An alert informs the IDS analyst that some interesting traffic has been observed. But it is after-the-fact because the traffic is not blocked or stopped in any way from reaching its destination."

Compare that to firewalls that block out known malware and intrusion prevention system (IPS) technology, which as the name describes, also blocks malicious traffic.

Although an IDS doesn't stop malware, cybersecurity experts said the technology still has a place in the modern enterprise.

"The functionality of what it does is still critically important," said Eric Hanselman, chief analyst with 451 Research. "The IDS piece itself is still relevant because at its core it's detecting an active attack."

However, cybersecurity experts said organizations usually don't buy and implement IDS as a standalone solution as they once did. Rather, they buy a suite of security capabilities or a security platform that has intrusion detection as one of many built-in capabilities.

Rob Clyde, board of directors vice chair ISACA, an association for IT governance professionals, and executive chair for the board at White Cloud Security Inc., agreed that intrusion detection is still a critical capability. But he said companies need to understand that an intrusion detection system requires maintenance and consider whether, and how, they'll support an IDS if they opt for it.

"Once you've gone down the path to say we're going to keep track of what's going on in our environment, you need someone to respond to alerts and incidents. Otherwise, why bother?" he said.

Given the work an IDS takes, he said smaller companies should have the capability but only as part of a larger suite of functions so they're not managing the IDS in addition to other standalone solutions. They should also consider working with a managed security service provider for their overall security requirements, as the provider due to scale can more efficiently respond to alerts. "They'll use machine learning or maybe AI and human effort to alert your staff to an incident or intrusion you truly have to worry about," he said.

"And at mid-size and larger companies, where you really need to know if someone is inside the network, you do want to have the additional layer, or additional layers, than just what's built into your firewall," he said.

3 challenges of managing an IDS

Intrusion detection systems do have several recognized management challenges that may be more work than an organization is willing or able to take on.

False positives (i.e., generating alerts when there is no real problem). "IDSs are notorious for generating false positives," Rexroad said, adding that alerts are generally are sent to a secondary analysis platform to help contend with this challenge.

This challenge also puts pressure on IT teams to continually update their IDSs with the right information to detect legitimate threats and to distinguish those real threats from allowable traffic. It's no small task, experts said.

“IDS systems must be tuned by IT administrators to analyze the proper context and reduce false-positives. For example, there is little benefit to analyzing and providing alerts on internet activity for a server that is protected against known attacks. This would generate thousands of irrelevant alarms at the expense of raising meaningful alarms. Similarly, there are circumstances where perfectly valid activities may generate false alarms simply as a matter of probability,” Rexroad said, noting that organizations often opt for a secondary analysis platform, such as a Security Incident & Event Management (SIEM) platform, to help with investigating alerts.

Staffing. Given the requirement for understanding context, an enterprise has to be ready to make any IDS fit its own unique needs, experts advised.

“What this means is that an IDS cannot be a one-size-fits all configuration to operate accurately and effectively. And, this requires a savvy IDS analyst to tailor the IDS for the interests and needs of a given site. And, knowledgeable trained system analysts are scarce,” Novak added.

Missing a legitimate risk. "The trick with IDS is that you have to know what the attack is to be able to identify it. The IDS has always had the patient zero problem: You have to have found someone who got sick and died before you can identify it," Hanselman said.

IDS technology can also have trouble detecting malware with encrypted traffic, experts said. Additionally, the speed and distributed nature of incoming traffic can limit the effectiveness of an intrusion detection system in an enterprise.

"You might have an IDS that can handle 100 megabits of traffic but you might have 200 megabits coming at it or traffic gets distributed, so your IDS only sees one out of every three or four packets," Hanselman said.

The future of intrusion detection systems

Hanselman said those limitations still don't invalidate the value of an IDS as a function.

"No security tool is perfect. Different products have different blind spots, so the challenge is knowing those blind spots," he explained. "I continue to think that IDS will be with us for a long time to come. There's still that basic value in being able to identify specific hostile traffic on the wire."

However, experts said this has some organizations rethinking the need for an IDS – even though today implementing the technology remains a security best practice.

"This tuning and analysis requires a significant amount of effort based on the number of alerts received. An organization may not have the resources to manage all devices in this capacity. Other organizations may conduct a more comprehensive threat assessment and decide not to implement IDS devices," Rexroad said, adding that the high number of **IDS false positives** have some organizations opting against implementing IPSs as well for fear of blocking legitimate business transactions.

He said other organizations may decide to focus on more advanced protections at the internet gateway or use flow analysis from network devices in conjunction with log analysis from systems and applications to identify suspect events instead of using an IDS.

IDS vs. IPS

Likewise, Scott Simkin, director of threat intelligence at Palo Alto Networks, said he does not believe IDS as a solution has a role in most modern enterprises.

But, he said, he said he does think IDS retains a place as a function in a broader cybersecurity portfolio.

“The capability is absolutely critical and foundational to every single security team,” he said, adding that the automation and intelligence being built into modern security platforms have pushed IDS as a function deeper into the solution.

“IDSs [as systems] been superseded by IPSs and next-generation firewalls that take the concept of IDS and then layer something on top of it. And those should exist alongside behavioral analytics, web filtering, application identity management and other controls,” he said. “But you don’t really buy IDSs anymore.”

IDS Usage in Networks

When placed at a strategic point or points within a network to monitor traffic to and from all devices on the network, an IDS will perform an analysis of passing traffic, and match the traffic that is passed on the subnets to the library of known attacks. Once an attack is identified, or abnormal behavior is sensed, the alert can be sent to the administrator.

IDS Evasion/Avoidance Techniques

Being aware of the techniques available to cyber criminals who are trying to breach a secure network can help IT departments understand how IDS systems can be tricked into not missing actionable threats:

- Fragmentation: Sending fragmented packets allow the attacker to stay under the radar, bypassing the detection system's ability to detect the attack signature.
- Avoiding defaults: A port utilized by a protocol does not always provide an indication to the protocol that’s being transported. If an attacker had reconfigured it to use a

different port, the IDS may not be able to detect the presence of a trojan.

- Coordinated, low-bandwidth attacks: coordinating a scan among numerous attackers, or even allocating various ports or hosts to different attackers. This makes it difficult for the IDS to correlate the captured packets and deduce that a network scan is in progress.
- Address spoofing/proxying: attackers can obscure the source of the attack by using poorly secured or incorrectly configured proxy servers to bounce an attack. If the source is spoofed and bounced by a server, it makes it very difficult to detect.
- Pattern change evasion: IDS rely on pattern matching to detect attacks. By making slight adjust to the attack architecture, detection can be avoided.