Intrusion Detection System

A powerful tool to identify and respond to potential security threats

Edited by **MOHAN DAS VISWAM**

Introduction

An Intrusion Detection System (IDS) is a device or software application used to monitor network traffic for indications of malicious activity. It analyses incoming network traffic, compares it to known attack signatures, and generates alerts when it detects malicious activity. As the volume and sophistication of cyber threats continue to increase, organisations require a reliable method to detect and respond to potential security breaches. An IDS provides the organisation with this capability.

Types of Intrusion Detection Systems

IDSs come in a variety of flavours and use a variety of detection methodologies to identify suspicious activities. They can be broadly classified into the following groups, on the basis of deployment environment:

- **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

- **Host Intrusion Detection System (HIDS)** runs on 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 an NIDS in that it may be able to detect anomalous network packets that originate from inside the organization or malicious traffic that an 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

Beyond their deployment location, IDS solutions also differ in how they identify potential intrusion and threats

- **Signature-based Intrusion Detection System (SIDS)** monitors all the packets traversing the network and compares them against a database of known signatures or attributes of known malicious threats, much like antivirus software. Attack signatures are patterns of network traffic that are associated with specific types of attacks. For example, an IDS might recognize that a certain pattern of network traffic is associated with a SQL injection attack or DNS poisoning and generate an alert when it detects that pattern.

- **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. 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. For example, if an IDS detects a sudden spike in traffic from a particular IP address, it might generate an alert, as this could be a sign of a DoS (Denial of Service) attack or an attempt for DNS poisoning.

Modern IDSs often employ a Hybrid approach which uses a combination of two or more

In the modern age of interconnected technology, where businesses and organizations rely heavily on networks to store and transmit sensitive information, the importance of a robust and efficient Intrusion Detection System (IDS) cannot be emphasized enough. An IDS is a critical security tool that aids in the detection and response to potential threats and attacks on an organization's network infrastructure. It helps in maintaining the confidentiality, integrity, and availability of the sensitive information and ensures the overall security of the network infrastructure.

C.J. Antony
Dy. Director General
& HoG
antony@nic.in

Abhishek Sisodia
Scientist-C
abhishek.sisodia@nic.in

detection techniques to increase their accuracy as well as range and scope of detection.

Once an IDS has detected suspicious activity, it will generate an alert. The alert will typically include information about the nature of the activity, the time it occurred, and the source and destination of the traffic. Security personnel can then use this information to investigate the incident further and take appropriate action to mitigate the threat.

Benefits

Intrusion Detection System offer organizations several benefits, starting with the ability to identify security incidents. IDS can be used to help analyse the quantity and types of attacks. Organizations can use this information to change their security systems or implement more effective controls and improving compliance. An Intrusion Detection System can also help companies identify problems with their network device configurations. These metrics can then be used to assess future risks and subsequently take preventive steps.

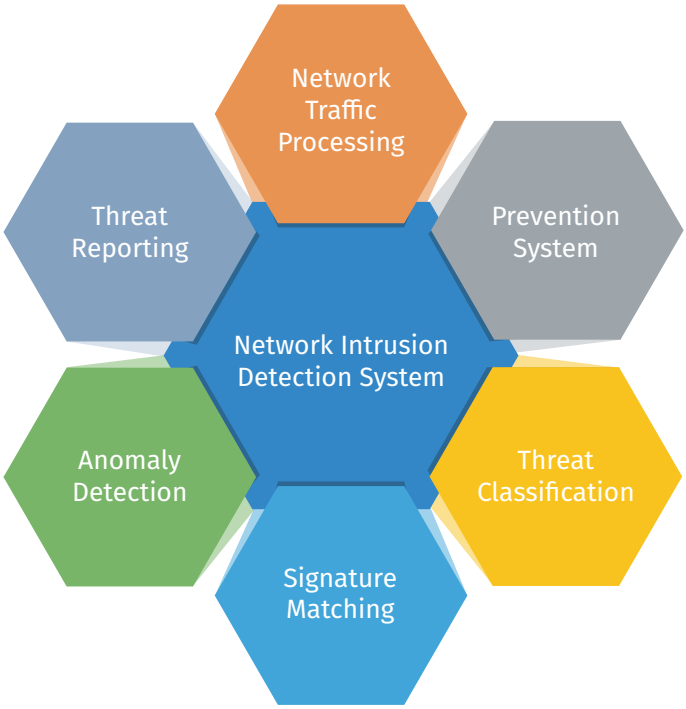
Intrusion Detection Systems can also help enterprises attain regulatory compliance. Businesses can use their IDS logs as part of the documentation to show they are meeting certain compliance requirements. Many industries are subject to strict data protection regulations, such as HIPAA (Health Insurance Portability and Accountability Act) in healthcare or PCI DSS (Payment Card Industry Data Security Standard) in finance. IDSs make it easier for organizations to meet these security regulations.

IDSs 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 services being used. Using IDS to collect this information can be much more efficient than manual censuses of connected systems to prepare SOPs and contingency plans.

Challenges

IDSs 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 tuning and 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 Intrusion Detection System to be over-sensitive to abnormal behaviors and generate false positives than it is to be under-sensitive, generating false negatives.



Network Intrusion Detection System

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

IDS Vs. IPS

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are two types of security solutions that are designed to protect networks from potential cyber threats. While they share some similarities, there are significant differences between the two.

An IPS is a security solution that goes beyond the capabilities of an IDS. In addition to monitoring network traffic, an IPS can take action to prevent potential threats from being executed. It does this by blocking traffic that is identified as potentially malicious, based on the policies and rules that are configured. IDSs are typically less expensive and less complex to deploy than IPSs.

However, IDSs require trained security personnel to investigate alerts and take appropriate action.

An IPS works by comparing network traffic against a database of known attack signatures, much like an IDS. However, when it detects a potential threat, along with generating an alert, it takes immediate action to prevent the threat from being executed. This action can include blocking traffic, dropping packets, or resetting connections.

Finally, there is a difference in the level of granularity between IDS and IPS. IDSs can be configured to monitor specific types of traffic, such as web traffic or email traffic, or they can be configured to monitor all network traffic. IPSs, on the other hand, are typically configured to block specific types of traffic, such as malware or phishing attempts, or they can be configured to block all traffic that is identified as potentially malicious.

Conclusion

An Intrusion Detection System is an essential component of modern cyber-security and act as a powerful tool for protecting against cyber attacks. To ensure that an IDS is effective, it is essential to regularly update its signatures and ensure that it is configured correctly. IDSs are not foolproof and can generate false positives, so it is important to have trained personnel who can investigate alerts and can tune IDS policies accordingly.

Contact for more details

Abhishek Sisodia
Scientist-C
Network Security Division, NIC Headquarters
CGO Complex, Lodhi Road, New Delhi - 110003
Email: abhishek.sisodia@nic.in, Phone: 011-24305747