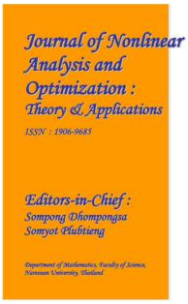


Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Issue. 1, No.4 : 2024
ISSN : **1906-9685**

INTRUSION DETECTION SYSTEM (IDS) IN NETWORKS

Mr. V. VEERAKUMARAN Assistant Professor, School of Commerce Nehru Arts and Science College (NASC), Nehru Gardens, Thirumalayampalayam, Coimbatore, Tamilnadu, India – 641 105
Mail Id: nascveerakumaran@nehrucolleges.com
Mr. GOKULPRASANTH.S Student, School of Commerce Nehru Arts and Science College (NASC), Nehru Gardens, Thirumalayampalayam, Coimbatore, Tamilnadu, India – 641 105.
Mr. KESAVAN.V Student, School of Commerce Nehru Arts and Science College (NASC), Nehru Gardens, Thirumalayampalayam, Coimbatore, Tamilnadu, India – 641 105.

ABSTRACT
Using network any user can share the portfolios resource like printer, CDs, USBs, Scanner, etc.., an/or help to authorize to communicate between electronic devices the electronic devices are connected by across radio waves, cables, infrared light beams, telephone lines, microwave and/or satellites etc.., There are many networks are some of them are Local Area Network, Wide Area Network, Metropolitan Area Network. Internet is otherwise known as "The Network of Networks." In one entity the computers are connected around the world. Hence here numerous networked computers are connected.
An IDS monitoring system which used to recognized the network traffic and seek for sceptical activities and encounters the observant when they are recognized. A security operations centre (SOC) responder can explore the problems based on the encounters and take the proper measurement to Intensifies the threat.

INTRODUCTION
An Intrusion Detection System (IDS) can automate the detection of network threats by alerting security administrators to recognized or potential risks, or by transmitting alerts to a centralized security tool. A centralized security tool, such as a Security Information and Event Management (SIEM) system, can combine data from various sources to aid security teams in identifying and responding to cyber threats that might evade other security measures.
Furthermore, IDSs can assist in compliance efforts. Regulations like the Payment Card Industry Data Security Standard (PCI-DSS) require organizations to implement intrusion detection measures.
However, it's important to note that an Intrusion Detection System alone cannot prevent security threats. Currently, IDS capabilities are typically integrated with or absorbed into intrusion prevention systems (IPSs), which can identify security threats and automatically take action to prevent them.

INTRUSION DETECTION SYSTEM WORKS
IDSs can appear as software applications installed on endpoints or dedicated hardware devices connected to the network. Some IDS solutions are available as cloud services. Despite its form, an IDS utilizes one or both of two primary threat detection methods: signature-based or anomaly-based detection.

- **SIGNATURE BASED AND DETECTION**

Signature-based detection analyses network packets for unique characteristics or behaviours associated with a specific threat. An example of such a characteristic is a piece of code found in a particular malware variant.
A signature-based IDS stores a collection of attack signatures to compare against incoming network packets. When a packet matches one of these signatures, the IDS detects it. To work effectively, signature databases need regular updates with new threat information to keep up with emerging cyber

threats and changes to existing ones. Newly developed attacks that haven't been analysed for signatures can evade detection by signature-based IDS systems.

- **ANOMOLY-BASED DETECTION**

Using machine learning, anomaly-based detection methods develop and continuously update a baseline model of typical network activity. This model is then used to compare ongoing network activity, identifying any deviations, such as a process consuming more bandwidth than usual or a device opening an unexpected port.

Anomaly-based IDSs are valuable because they can detect new cyberattacks that may bypass signature-based detection. For instance, they can identify zero-day exploits, which exploit software vulnerabilities before developers are aware of them or have time to patch them.

However, anomaly-based IDSs may generate more false positives. Even legitimate actions, like an authorized user accessing a sensitive network resource for the first time, might trigger an alert from an anomaly-based IDS.

LESS COMMON DETECTION METHODS

When an IDS identifies a possible threat or breach of policy, it notifies the incident response team for further investigation. Various methods, including reputation-based detection and stateful protocol analysis, are employed to block traffic from IPs and domains linked to suspicious activities. IDSs maintain records of security incidents, either internally or through a SIEM tool, which can be utilized to enhance criteria by incorporating new attack signatures or refining network behaviour models.

TYPES OF INTRUSION PREVENTION SYSTEM

- HIDS
- NIDS
- PIDS
- APIDS
- **Network intrusion detection systems (NIDSs)** observe incoming and outgoing traffic to devices throughout the network. Positioned strategically, typically right after firewalls at the network edge, NIDSs can detect any unauthorized traffic that penetrates defences.

Additionally, NIDSs may be positioned internally to identify insider threats or compromised user accounts. For instance, NIDSs could be situated behind each internal firewall within a segmented network to monitor traffic between subnets.

To prevent hindrance to legitimate traffic flow, NIDSs are often deployed "out-of-band," where traffic doesn't pass directly through them. Instead, NIDSs analyse copies of network packets, ensuring that legitimate traffic is not delayed while still enabling the detection and flagging of malicious activity.

- **Host intrusion detection systems (HIDSs)** are deployed on specific endpoints, such as laptops, routers, or servers. These systems exclusively monitor activity on the designated device, including incoming and outgoing traffic. HIDSs typically function by periodically capturing snapshots of critical operating system files and then comparing these snapshots for any changes over time. If a HIDS detects alterations, such as edits to log files or modifications to configurations, it promptly alerts the security team.

Security teams often integrate both network-based intrusion detection systems and host-based intrusion detection systems. While the NIDS scrutinizes overall network traffic, the HIDS provides additional defense for valuable assets. Moreover, a HIDS can aid in identifying malicious activities originating from a compromised network node, such as the spread of ransomware from an infected device.

- Security teams can utilize various IDSs beyond the typical NIDS and HIDS for specialized purposes. One such option is a **Protocol-based IDS (PIDS)**, which monitors connection protocols between servers and devices. PIDS are frequently positioned on web servers to oversee HTTP or HTTPS connections. Additionally, there's the **Application protocol-based IDS (APIDS)**, which operates at the application layer, scrutinizing application-specific protocols. Typically, an APIDS is deployed between a web server and an SQL database to identify SQL injections.

Although IDS solutions possess the capability to identify numerous threats, hackers possess the ingenuity to circumvent them. In response, IDS vendors continuously refine their solutions to counter these tactics. Nonetheless, this cycle of solution updates fosters an arms race dynamic, wherein hackers and IDSs vie to outmanoeuvre each other.
Numerous tactics are employed by hackers to evade IDS detection, including:
1. **Distributed Denial-of-Service (DDoS) Attacks**: This involves inundating IDSs with malicious traffic from various sources to overwhelm their resources. This flooding of decoy threats enables hackers to exploit vulnerabilities while the IDS is preoccupied.
2. **Spoofing**: By falsifying IP addresses and DNS records, hackers can create the illusion that their traffic originates from a reputable source, thus eluding detection.
3. **Fragmentation**: Malware or malicious payloads are divided into smaller packets, obscuring their signatures and evading detection. Through strategic packet delays or out-of-order transmission, hackers can thwart IDS reassembly attempts, concealing their attacks.
4. **Encryption**: Utilizing encrypted protocols allows hackers to bypass IDS detection, provided the IDS lacks the requisite decryption key.
5. **Operator Fatigue**: Intentionally generating a plethora of IDS alerts serves to distract incident response teams from the hackers' actual activities.

IDS SECURITY SOLUTIONS

IDSs do not operate independently; instead, they are crafted to function within a comprehensive cybersecurity framework and frequently intertwine with one or more of the subsequent security solutions.

IDS and SIEM

IDS alerts are typically directed towards an organization's **Security Information and Event Management (SIEM)** system, where they can be amalgamated with alerts and data from various other security utilities, consolidating them into a unified dashboard. This integration of IDS with SIEM platforms empowers security teams to enhance IDS alerts using threat intelligence and information derived from other tools, discern false positives, and determine incident prioritization for remedial action.

DIFFERENCE BETWEEN IDS and IPS

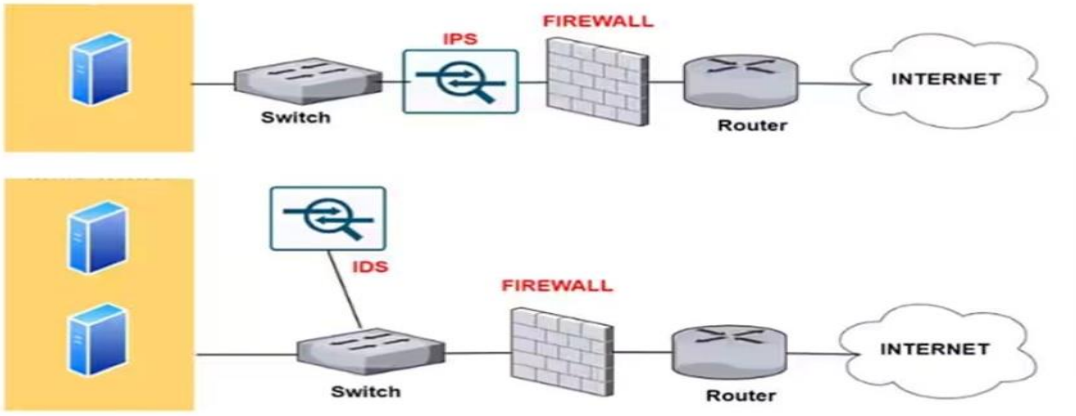
The following table summarizes the differences between the IPS and the IDS deployment

		Intrusion Prevention System	**IDS Deployment**
Placement network in infrastructure		Part of the direct line of communication (inline)	Outside direct line of communication (out-of-band
System Type		Active (monitor & automatically defend) and/or passive	Passive (monitor & notify)
Detection mechanisms	1. Statistical anomaly-based detection 2. Signature detection: - Exploit-facing signatures - Vulnerability-facing signatures	1. Signature detection: - Exploit-facing signatures	
Flexibility	Offers more flexibility for network administrators to investigate and respond to threats manually	Provides less flexibility as it automatically blocks or mitigates threats based on predefined rules.	

Use cases	Useful for monitoring and analyzing network traffic for security breaches, compliance, and forensic analysis.	Ideal for networks requiring real-time protection against known and emerging threats, such as critical infrastructure or high-security environments.

IDS FIREWALLS

IDSs and firewalls play complementary roles in network security. Positioned at the network perimeter, firewalls serve as protective barriers, employing predefined rulesets to regulate incoming and outgoing traffic. IDSs, typically situated in close proximity to firewalls, serve as a secondary line of defense, detecting and flagging any malicious activity that bypasses the firewall. Certain firewalls, particularly next-generation variants, integrate IDS and IPS functionalities seamlessly.



Diagram

CONCLUSION

In conclusion, Intrusion Detection Systems (IDSs) are vital components of a comprehensive cybersecurity strategy, assisting in threat detection, compliance adherence, and incident response. Whether employing signature-based or anomaly-based detection methods, IDSs play a crucial role in identifying and mitigating cyber threats. However, they operate most effectively when integrated with other security solutions such as SIEM platforms and firewalls, forming a cohesive defense against evolving attack tactics. Despite the ongoing arms race between hackers and IDS vendors, the continuous refinement of IDS solutions underscores their importance in safeguarding network integrity and data confidentiality. Integrating IDSs with SIEM systems enhances threat intelligence utilization and facilitates efficient incident response, ultimately bolstering organizational resilience against cyber threats.

REFERENCES

- Biswanath Mukherjee, L. Todd Heberlein, and Karl N. Levitt. Network intrusion detection. IEEE Network, 8(3):26-41, May/June 1994.
- Gregory B. White, Eric A. Fisch, and Udo W. Pooch. Computer System and Network Security. CRC Press Inc., 1996.
- B. Le Charlier, A. Mounji, M. Swimmer. Dynamic Detection and Classification of Computer Viruses Using General Behaviour Patterns. In Proceedings of Fifth International Virus Bulletin Conference. September 20-22, 1995.
- Tsudik, G. and Summers, R. AudES - an expert system for security auditing. In Proceedings of the AAAI Conference on Innovative Applications in AI, May 1990.