TECHNICAL REPORT WRITING

Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)

NAME: RUPAK SARKAR

ROLL NO.: 14271024036

STREAM: MASTER OF COMPUTER APPLICATION

SUBJECT NAME: INTRODUCTION TO CYBER SECURITY

SUBJECT CODE: MCAN-E205D

COLLEGE NAME: MEGHNAD SAHA INSTITUTE OF TECHNOLOGY

UNIVERSITY NAME: MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY

ABSTRACT

This technical report delves into the core principles of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) in cyber security. It offers a comprehensive analysis of how these systems safeguard networks by monitoring for unauthorized access, detecting malicious activities, and mitigating cyber threats. The report explores the architecture and functionality of IDS and IPS, emphasizing their roles in identifying, analyzing, and countering security breaches. Furthermore, it highlights the distinctions between detection and prevention mechanisms while addressing challenges in implementation, such as false positives, performance impact, and evolving attack vectors. The findings underscore the vital role of IDS and IPS in enhancing cybersecurity defenses and maintaining the integrity and security of modern computing environments.

CONTENTS

INTRODUCTION

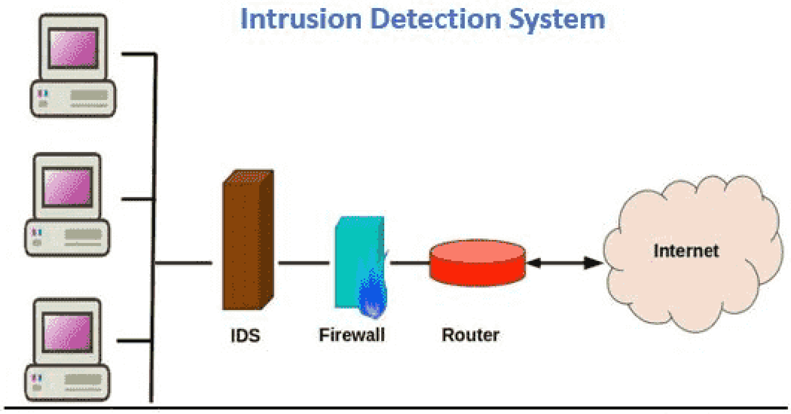
In the ever-evolving realm of cybersecurity, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) serve as vital defenses against malicious threats. IDS functions by continuously monitoring network traffic and system activities, detecting potential security breaches through anomaly detection and signature-based analysis. On the other hand, IPS goes beyond detection by actively preventing attacks, blocking, or mitigating harmful traffic in real time. These systems are indispensable for organizations seeking to safeguard sensitive data, prevent unauthorized access, and uphold network integrity.

The efficiency of IDS and IPS relies on proper deployment, configuration, and their ability to adapt to evolving threats. This report investigates the core principles, architectures, and operational mechanisms of IDS and IPS, emphasizing their importance in contemporary cybersecurity frameworks. Furthermore, it addresses challenges such as false positives, resource limitations, and the necessity for continuous updates to combat advanced cyber threats.

TECHNICAL REPORT

Intrusion Detection System (IDS)

An Intrusion Detection System (IDS) is a cybersecurity solution designed to continuously monitor network traffic and system activities for indicators of potential security breaches or malicious behavior. By analyzing data patterns, it identifies unauthorized access, suspicious activities, or policy violations and promptly alerts administrators to potential threats. Primarily focused on threat detection and early warning, IDS enables organizations to respond proactively to attacks, mitigating risks before significant damage occurs.



Classification of Intrusion Detection Systems –

Network Intrusion Detection System (NIDS):

A **Network Intrusion Detection System (NIDS)** is strategically deployed within a network to monitor and analyze traffic from all connected devices. It observes data packets passing through the entire subnet and compares them against a database of known attack signatures. When an attack is detected or abnormal behavior is identified, an alert is generated and sent to the administrator for further investigation. For instance, a NIDS can be installed on a subnet where firewalls are located to detect attempts to bypass or compromise the firewall.

Host Intrusion Detection System (HIDS):

A **Host Intrusion Detection System (HIDS)** operates on individual hosts or devices within a network, monitoring incoming and outgoing traffic specific to that device. It detects suspicious or malicious activity and alerts the administrator when anomalies are identified. HIDS works by taking snapshots of system files and comparing them with previous versions. If any critical files have been modified or deleted, an alert is triggered for further investigation. This type of system is particularly useful for mission-critical machines that are expected to remain unchanged, ensuring their integrity and security.

Protocol-based Intrusion Detection System (PIDS):

A **Protocol-based Intrusion Detection System (PIDS)** is a security mechanism that operates at the front end of a server, analyzing the communication protocols between users, devices, and the server. It is specifically designed to monitor and interpret protocol traffic, such as the HTTPS protocol stream, to detect anomalies and potential security threats. By continuously observing these interactions, a PIDS helps secure web servers by identifying malicious activity within protocol exchanges. Since HTTPS traffic is encrypted, the system must be positioned at the interface where HTTPS transitions to unencrypted HTTP before reaching the web presentation layer.

Application Protocol-based Intrusion Detection System (APIDS):

An **Application Protocol-based Intrusion Detection System (APIDS)** is a security system or agent deployed within a group of servers to monitor and analyze communication over application-specific protocols. It detects intrusions by interpreting protocol interactions at the application layer, ensuring the integrity and security of critical operations. For instance, an APIDS can monitor SQL protocol communications between middleware and a database on a web server, identifying suspicious queries or unauthorized access attempts.

Hybrid Intrusion Detection System (HIDS):

A **Hybrid Intrusion Detection System (HIDS)** integrates multiple intrusion detection approaches to provide a comprehensive security solution. By combining host-based data with network traffic analysis, it offers a holistic view of the network environment, enhancing detection accuracy and response capabilities. This fusion of host and network information allows for better identification of security threats, reducing false positives and improving overall effectiveness. Compared to standalone IDS types, a hybrid IDS delivers enhanced threat visibility and protection.

Detection methods of IDS –

Anomaly-based Method:

Anomaly-based Intrusion Detection Systems (IDS) were developed to identify unknown malware attacks, addressing the challenge of rapidly evolving threats. This approach utilizes machine learning to establish a baseline model of normal system behavior. Incoming activities are then compared against this model, and any deviations are flagged as suspicious. Unlike signature-based IDS, which relies on predefined attack patterns, anomaly-based IDS offers greater adaptability.

Signature-based Method:

A Signature-based Intrusion Detection System (IDS) identifies attacks by analyzing specific patterns in network traffic, such as the number of bytes, sequences of 1’s and 0’s, or known malicious instruction sequences used by malware. These predefined patterns, known as signatures, enable the system to recognize and block threats that have already been documented. While highly effective at detecting known attacks, this method struggles to identify new or emerging malware, as their signatures are not yet recorded in the system.

Advantages of IDS –

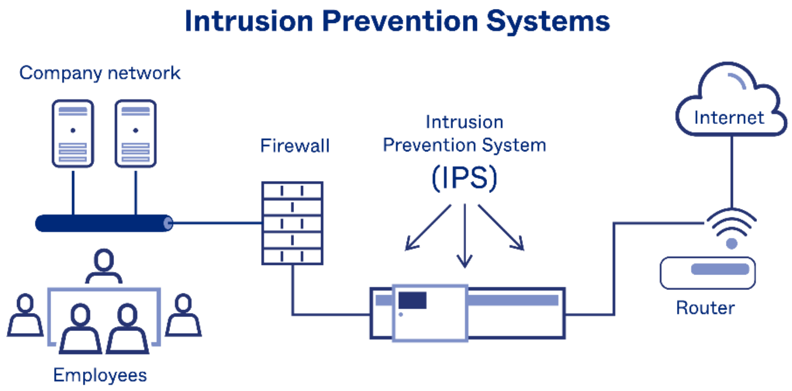
- It keeps a check on all the incoming and outgoing network activity. It detects any signs of intrusion in the system. Its main function is to send an alert immediately when it identifies any activity in the system.
- It recognizes various security incidents. Also helps to examine the quantity and types of such suspicious attacks. It also detects bugs and issues relating to their network device configurations
- IDS sensors identify hosts and other network devices. They tend to examine the data within the network and the operating system. This saves the time of the IT team. Thus, the efficiency of the organization increases. This will help the organization to cut off the staff cost.
- IDS can also be used as a tool to meet certain requirements. They offer transparency across your network. Thus, it helps the organization to meet with different regulations for security.

Disadvantages methods of IDS –

- At times they might send some false alarms. Thus, an organization needs to detect such things when they are first using it. They need to configure the system so that they can easily identify normal traffic. They can easily distinguish any malicious activity.
- Such false alarms sometimes can create some serious issues. IDS might skip a threat to such recognized traffic. In such a scenario, the IT teams have no sign that an attack might take place. Thus, they will fail to take any steps. Thus, it is advisable to be careful about such abnormal behaviors.
- IDS help to monitor the network. But they don't block or resolve such issues. The organization needs to hire the right personnel to look after such threats and take immediate action.
- Intrusion Detection Systems are suffering from a serious issue. They fail to detect a new suspected intrusion, as the new malware does not display the pattern of previous unusual behavior. Thus, the IDS must take steps to detect such new behavior. So that an organization can take immediate precautions to such a threat.

Intrusion Prevention System (IPS)

An Intrusion Prevention System (IPS) is a proactive security solution that continuously monitors network traffic and system activities to detect and prevent malicious attacks in real time. Unlike an Intrusion Detection System (IDS), which only alerts administrators to potential threats, an IPS takes immediate action to block or mitigate harmful traffic before it reaches its target. By actively preventing unauthorized access, data breaches, and other security threats, an IPS plays a crucial role in maintaining network integrity and protecting sensitive information.



Classification of Intrusion Detection Systems –

Network-Based Intrusion Prevention System (NIPS):

A **Network-Based Intrusion Prevention System (NIPS)** continuously monitors network traffic to detect and prevent suspicious activities by analyzing protocol behavior. It inspects both network and application-layer protocols to identify potential threats and malicious activities. NIPS can detect a wide range of security incidents, making it a critical defense mechanism. Typically, it is deployed at key network boundaries, such as near firewalls, routers, remote access servers, and wireless networks, to provide real-time protection against cyber threats.

Wireless Intrusion Prevention System (WIPS):

A **Wireless Intrusion Prevention System (WIPS)** is designed to monitor and protect wireless networks by analyzing wireless networking protocols for suspicious activity. Unlike other intrusion prevention systems, WIPS focuses specifically on detecting threats and anomalies within wireless communication protocols rather than higher-layer network protocols like TCP or UDP. Typically deployed within an organization's wireless network range, WIPS helps detect unauthorized access points, rogue devices, and other wireless security threats. It can also be strategically placed in areas where unauthorized wireless activity might occur, ensuring comprehensive protection against wireless-based intrusions.

Network Behavior Analysis (NBA):

Network Behavior Analysis (NBA) is a security approach that examines network traffic to detect anomalies and identify potential threats based on unusual traffic patterns. It is particularly effective in detecting distributed denial-of-service (DDoS) attacks, certain types of malwares (such as worms and backdoors), and policy violations, such as unauthorized network services running on client systems. NBA systems are primarily deployed to monitor internal network traffic but can also be positioned to observe traffic between an organization's network and external entities, such as the Internet or business partners' networks. By analyzing deviations from normal traffic behavior, NBA enhances network security by detecting and mitigating threats in real time.

Host-Based Intrusion Prevention System (HIPS):

A **Host-Based Intrusion Prevention System (HIPS)** is a security software package installed on an individual host to detect and prevent suspicious activity by analyzing events occurring within that system. It monitors various characteristics, including network traffic (specific to the host), system logs, running processes, application activity, file access and modifications, and changes to system or application configurations. HIPS is most commonly deployed on critical hosts, such as publicly accessible servers and systems containing sensitive information, to provide an additional layer of protection against cyber threats. By actively detecting and responding to anomalies, HIPS enhances the security of individual devices within a network.

Detection methods of IPS –

Signature-based detection:

Signature-based IDS operates packets in the network and compares with pre-built and preordained attack patterns known as signatures.

Statistical Anomaly-Based Detection:

Statistical anomaly-based Intrusion Detection Systems (IDS) monitor network traffic and compare it against a predefined baseline of normal activity. This baseline is established by analyzing typical network behavior, including commonly used protocols and traffic patterns. Any deviations from this expected behavior are flagged as potential threats. However, if the baseline is not accurately configured, the system may generate false alarms, mistakenly identifying legitimate activities as security threats.

Stateful protocol analysis detection:

This IDS method recognizes divergence of protocols stated by comparing observed events with pre-built profiles of generally accepted definitions of not harmful activity.

Advantages of IPS –

- **Protects networks**: IPS detects and blocks cyber threats like malware, unauthorized access, and zero-day exploits.
- **Reduces risk of data breaches**: IPS enforces security policies to prevent potential attacks.
- **Reduces downtime**: IPS helps prevent network and system downtime.
- **Uses threat intelligence**: IPS automatically uses threat intelligence to keep up with the speed of attacks.

Disadvantages of IPS –

- **False positives**: IPS may block normal traffic as a threat, which can cause network disruptions.
- **Network performance**: IPS can slow down networks by analyzing and blocking traffic.
- **Cost**: IPS implementation and maintenance can be expensive.
- **Threat detection**: IPS can't detect new threats without signature updates.
- **DoS attacks**: IPS can create opportunities for DoS attacks when it stops non-malicious activity.
- **Network connectivity**: When multiple IPSes are linked, network connectivity can be poor.

Feature	Intrusion Detection System (IDS)	Intrusion Prevention System (IPS)
Functionality	Monitors and detects suspicious network activity.	Monitors, detects, and actively blocks threats.
Response	Alerts administrators but does not take direct action.	Automatically takes action to prevent or mitigate threats.
Placement	Typically placed inside the network to analyze traffic.	Usually positioned in-line with network traffic to block malicious activity.
Effect on Traffic	Passively observes and analyzes traffic.	Actively intervenes, which may slightly impact network performance.
False Positives	False positives may generate unnecessary alerts.	Incorrect blocking may disrupt legitimate traffic.

CONCLUSION

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) play a crucial role in modern cybersecurity by helping organizations identify and counter potential threats. While IDS focuses on monitoring network activity and generating alerts without directly intervening, IPS actively prevents malicious actions by blocking harmful traffic.

Both systems contribute to strengthening network security; however, their effectiveness depends on proper configuration, regular updates, and optimization. Although challenges such as false positives and high resource consumption exist, IDS and IPS remain essential for preventing cyber threats.

With the continuous evolution of cyberattacks, integrating IDS and IPS with advanced technologies such as artificial intelligence and machine learning can enhance threat detection and response, further fortifying cybersecurity defenses.

ACKNOWLEDGEMENT

I would like to acknowledge all those without whom this project would not have been successful. Firstly, I would wish to thank my teacher Mrs. Reshmi Maulik who guided me throughout the project and gave her immense support. She made us understand how to successfully complete this project and without her, the project would not have been complete.

This project has been a source to learn and bring our theoretical knowledge to the real-life world. So, I would really acknowledge her help and guidance for this project.

I would also like to thank my parents who have always been there whenever needed. Once again, thanks to everyone for making this project successful.