NETWORK INTRUSION DETECTION SYSTEM

Group-9

DILIP GOUD VATNALA

SAI TEJA MUNJA

MARUTHI SAI LINGAMPALLI

AASREETHAA SAGGU

Manasa Cherukupally

INTRODUCTION

- Network Intrusion Detection System(NIDS) aims to detect and respond to security incidents quickly.
- Threats can cause serious damage to organizations, including data theft, financial losses, and legal liability.
- A NIDS monitors network traffic for suspicious activity.
- NIDS enables organizations to act quickly to prevent security incidents.
- NIDS helps organizations comply with network security regulations.
- NIDS can help organizations demonstrate compliance with data security regulations by providing additional protection against network threats.
- NIDS aims to improve network security by detecting and responding to potential threats in a proactive and effective manner.

What is network intrusion detection systems?

- A network intrusion detection system (NIDS) is a piece of security software or hardware that analyzes network traffic for signals of unauthorized access, mismanagement, or malicious behavior.
- It analyzes traffic in real time and compares it to known attacks or suspicious behavior patterns. It alerts security professionals or takes automatic steps, such as blocking or quarantining the source of the traffic if it finds any anomalies.
- NIDS is an important component of a comprehensive network security strategy since they aid in the detection and prevention of cyberattacks and other security risks.

Use case of network intrusion detection systems

- **Forensic Analysis:** NIDS logs can be used for forensic analysis in the event of a security breach. data can help identify the source of an attack and provide valuable insights into the attacker's methods and motives.

Use case of network intrusion detection systems

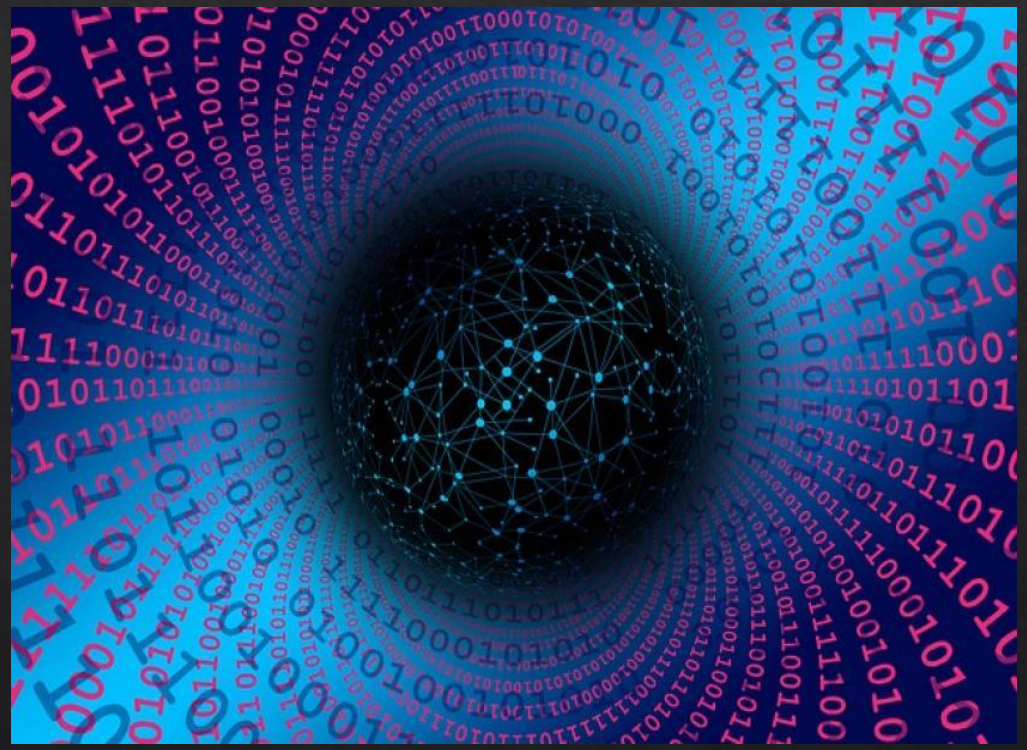
Protection of vital Infrastructure: Using NIDS, vital infrastructure may be monitored and secured against cyberattacks, including transportation networks, power grids, and financial networks.

Use case of network intrusion detection systems

Protection against Advanced Persistent Threats: Advanced persistent threats (APTs), which are complex assaults intended to avoid conventional security measures, may be found and prevented using NIDS.

Use case of network intrusion detection systems

Network Visibility: NIDS gives security personnel a thorough picture of network traffic, enabling them to see trends and abnormalities that can point to a security breach or data leak.

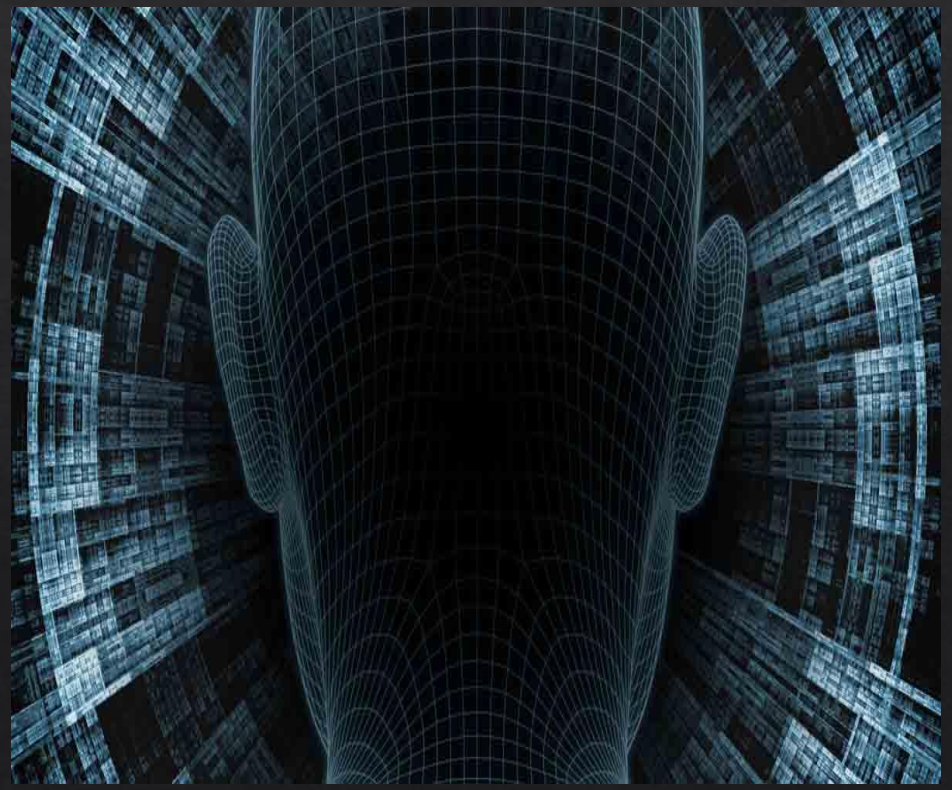


Network intrusion detection systems applications in Cybersecurity

- **Threat detection**: NIDS are used to detect potential threats and attacks on a network. They analyze network traffic and alert security personnel when they detect malicious traffic.
- **Incident response**: When a security incident occurs, NIDS can provide valuable information to help security personnel respond quickly and appropriately. NIDS can identify the source of an attack and the extent of the damage caused.
- **Compliance**: NIDS can help organizations meet regulatory compliance requirements. For example, the Payment Card Industry Data Security Standard (PCI DSS) requires the use of NIDS to protect credit card data.

Network intrusion detection systems **applications in Cybersecurity**

- **Network forensics:** NIDS can be used to capture and analyze network traffic for forensic purposes. This can be helpful in investigating security incidents and identifying the source of an attack.
- **User monitoring:** NIDS can be used to monitor user activity on a network. This can help organizations identify unauthorized access attempts and insider threats.
- **Threat intelligence:** NIDS can be used to gather threat intelligence by analyzing network traffic patterns and identifying new and emerging threats. This can help organizations stay ahead of potential attacks.



Confidentiality

According to Fortinet (n.d.) the initiatives taken by an organization to keep its data confidential are referred to as confidentiality. Fortinet (n.d.) also states that in order to accomplish this, information accessibility must be restricted to prevent the intentional or unintentional sharing of data with unauthorized parties.

Integrity

Fortinet (n.d.) mentions integrity involves making sure your data is trustworthy and unaltered. Fortinet (n.d.) states only if the data is trustworthy, precise, and valid will the integrity of the data be preserved. One may utilize a hashing, digital certificates, or digital signatures in order to maintain the trustworthy nature of the data (Fortinet, n.d.) .

Availability

Fortinet (n.d.) says although the data is kept private and its integrity is upheld, unless it is accessible to individuals within the business and the clients they serve, it is frequently meaningless. Fortinet (n.d.) mentions this requires that all systems, networks, and applications operate properly and at the appropriate times. Additionally, those who have access to certain information must be able to use it when they need to, and accessing the data shouldn't take too long (Fortinet, n.d.) .

Pros of Network intrusion detection systems in Cybersecurity

1. Continuous Monitoring IDS continuously monitors every specific computer network for any intrusion, breach, or suspicious activity (Rapid7, 2017).

2. To raise the alert and deliver notifications, it maintains a watchful eye on routers, firewalls, important servers, and files (Rapid7, 2017).

3. Rapid7 (2017) mentions IDS can be tuned to certain network packet content. A NIDS can be set to display only specific information within the packets, in addition to the ports and IP addresses that are utilized between two hosts, which a firewall may be able to display. With the use of this, intrusions like exploitation attacks or compromised endpoint devices that are a part of a botnet can be found (Rapid7, 2017).

4. IDS Qualifies and Quantifies Attacks The frequency and nature of attacks are analyzed by an IDS. One can modify their security systems or put new, more efficient controls in place using this knowledge (Rapid7, 2017).

5. They Help in Compliant with Regulation IDS make it simpler to adhere to security laws since they give you more visibility across your network and also your IDS logs can also be used in the documentation to satisfy certain standards (Rapid7, 2017).

Cons of Network intrusion detection systems in Cybersecurity

1. They cannot prevent incidents. An IDS just assists in identifying attacks; it does not stop or hinder them (Rapid7, 2017).
2. A busy network may make it difficult for NIDS to capture every packet, which could lead them to miss an assault conducted during a time of high traffic (Rapid7, 2017).
3. According to Rapid7 (2017), they are more prone to protocol-based attacks. The same protocol-based attacks that affect network hosts are also used against NIDS since they evaluate protocols as they are recorded (Rapid7, 2017).

Real Life Examples

- **Target breach:**

In 2013, Target experienced a massive data breach in which hackers stole credit and debit card information from millions of customers. The breach was detected by a NIDS, which alerted Target's security team to the suspicious activity. Unfortunately, Target's security team failed to act on the alert, allowing the attackers to continue their activities for several weeks.

- **WannaCry ransomware attack:**

In 2017, the WannaCry ransomware attack infected hundreds of thousands of computers in more than 150 countries. The attack was detected by a NIDS, which alerted security teams to the suspicious activity. The NIDS allowed security teams to quickly isolate infected machines and prevent the spread of the malware.

Real Life Examples

- **Equifax breach:**

In 2017, Equifax experienced a massive data breach in which hackers stole personal information from millions of customers. The breach was detected by a NIDS, which alerted Equifax's security team to the suspicious activity. Unfortunately, Equifax failed to act on the alert, allowing the attackers to continue their activities for several months.

- **SolarWinds supply chain attack:**

In 2020, a sophisticated supply chain attack affected multiple organizations worldwide, including several U.S. government agencies. The attack was detected by a NIDS, which alerted security teams to the suspicious activity. The NIDS allowed security teams to quickly identify and isolate affected systems.

Conclusion

In the cyber world, the assets are being protected with the early detection of the threat in any scenario, with network based intrusion detection system we can detect and then report the mode of intrusion method and medium to the security team and it can be responded respectively in a counter way in any stages of the system protection in any organization.

References

- https://www.rapid7.com/blog/post/2017/01/11/the-pros-cons-of-intrusion-detection-systems/
- https://www.fortinet.com/resources/cyberglossary/cia-triad
- https://www.geeksforgeeks.org/intrusion-detection-system-ids/amp/

Thank You