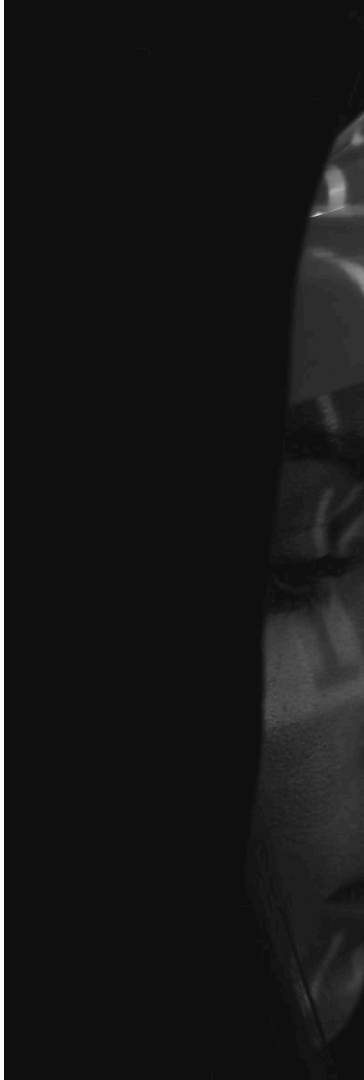

Intrusion
Detection
Systems
(IDS)

Intrusion Detection Systems (IDS)

- Intrusion Detection Systems (IDS) are security tools designed to monitor network or system activities and detect any unauthorised or malicious activities.
- They play a crucial role in safeguarding computer networks from potential threats or attacks.
- This presentation will provide an overview of IDS, focusing on the differences between host-based and network-based IDS, IDS sensors, and specific traffic types.

Host-Based IDS

- Host-based IDS (HIDS) operates on individual hosts or endpoints, analyzing the activities occurring on the host.
- Monitors logs, system calls, file integrity, and other host-specific data sources to detect any signs of intrusion.
- HIDS provides detailed information about activities occurring within a specific host, making it effective for detecting local attacks or unauthorized access to the host.



Network-Based IDS

Network-based IDS (NIDS):

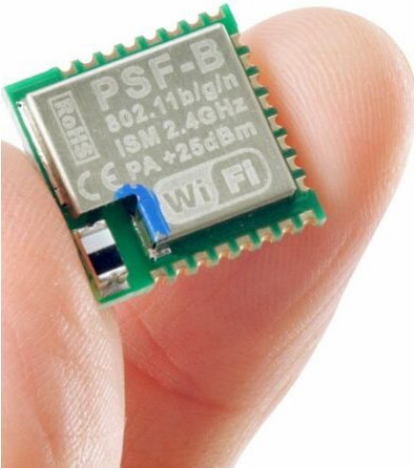
- Monitors network traffic
- Analyse packets and headers to identify any suspicious or malicious activities.

NIDS sensors are strategically placed within the network infrastructure to capture and inspect network traffic.

NIDS focuses on detecting attacks that traverse the network, such as:

- Network scanning
- Port scanning
- Denial-of-service attacks

IDS Sensors



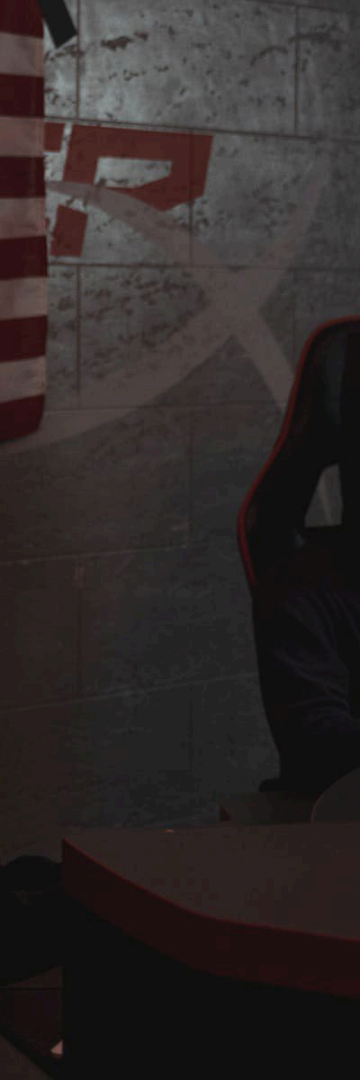
IDS sensors are the core components of an IDS system.

Responsible for collecting and analysing data to detect potential intrusions.

Sensors can be hardware-based, software-based, or a combination of both.

Hardware sensors are typically placed at network entry points, while software sensors can be installed on individual hosts or within virtual environments.

Analyse network traffic, system logs, and other relevant data sources to identify potential threats.



Signature-Based IDS

Signature-based IDS relies on a database of known attack signatures or patterns.

Compares network traffic or host activities against these signatures to identify any matches indicating a potential intrusion.

Signature-based IDS are effective at detecting well-known attacks, but they may struggle with detecting new or unknown threats.

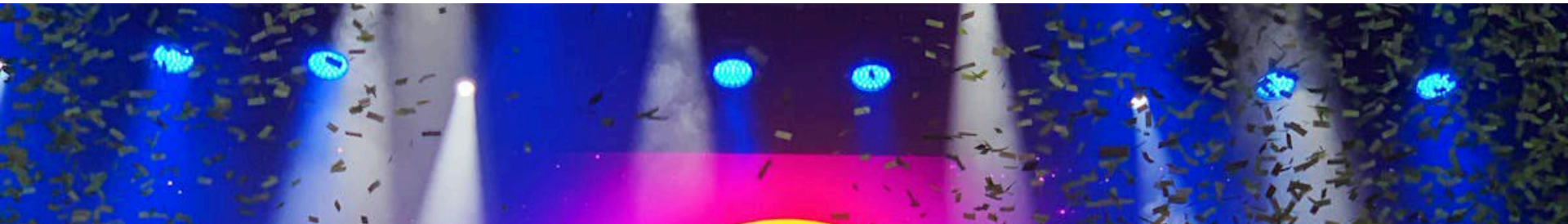
Regular updates of signature databases are crucial to ensure effectiveness.

Anomaly-Based IDS

Anomaly-based IDS focuses on identifying abnormal or unusual behavior that may indicate an intrusion.

Establishes a baseline of normal network or host activities and raises alerts when deviations from this baseline occur.

Anomaly-based IDS can detect novel attacks or zero-day vulnerabilities but may also generate false positives due to legitimate changes in network or system behavior.

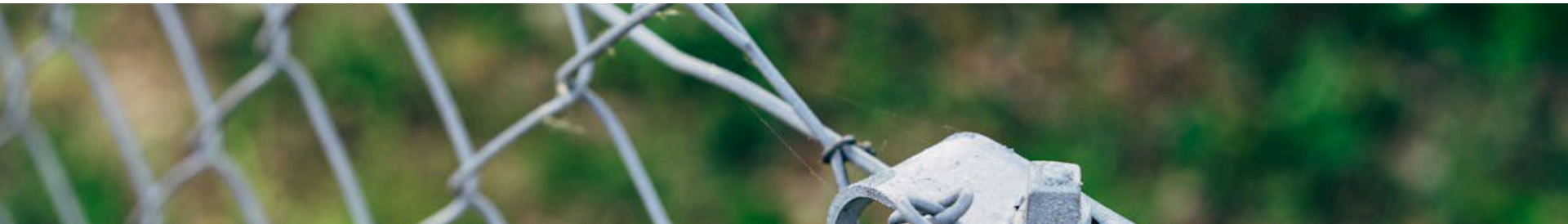


Hybrid IDS

Hybrid IDS combines the strengths of both signature-based and anomaly-based detection methods.

Uses signature databases to detect known attacks and anomaly detection techniques to identify suspicious or abnormal behavior

This approach provides a more comprehensive and accurate detection capability, reducing false positives and improving the detection rate for both known and unknown threats.



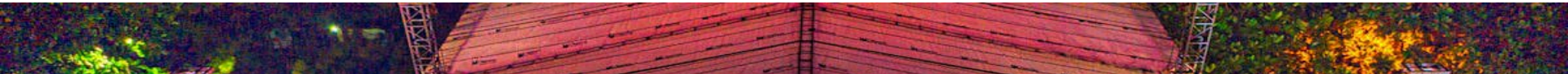
IDS Deployment Considerations

When deploying an IDS, several factors should be considered.

These include:

- Network topology
- Sensitivity of assets being protected
- Traffic volume
- Required level of intrusion detection

Proper placement of IDS sensors, careful configuration, and regular updates are essential to ensure the effectiveness of the IDS system.



IDS Alert Management

IDS systems generate alerts when potential intrusions are detected.

Efficient alert management is crucial to ensure that legitimate threats are promptly addressed while minimizing the impact of false positives.

Dedicated personnel, well-defined response procedures, and integration with incident response systems are key components of effective IDS alert management.

IDS Log Analysis

IDS logs provide valuable information about detected threats, network activities, and system events.

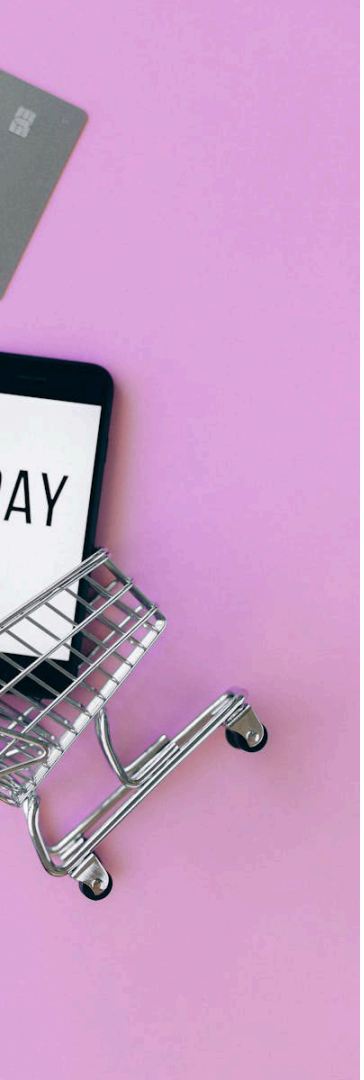
Analysing IDS logs can help identify attack patterns, determine the severity of incidents, and provide insights for future security enhancements.

Automated log analysis tools and correlation techniques can aid in extracting meaningful information from the vast amount of IDS log data.

Network Traffic Types

IDS systems need to analyze different types of network traffic to effectively detect intrusions. Traffic types include TCP/IP, UDP, ICMP, DNS, HTTP, FTP, and more.

Each traffic type has its own characteristics, protocols, and potential vulnerabilities. Understanding these traffic types enables IDS systems to focus on detecting specific attack vectors associated with each type.



HTTP Traffic Analysis

HTTP (Hypertext Transfer Protocol) is used for web communication.

IDS systems analyse HTTP traffic to detect web-based attacks. Such as:

- SQL injection
- Cross-site scripting (XSS)
- File inclusion vulnerabilities
- Other web application attacks

Monitoring HTTP traffic helps identify potential threats targeting web servers or web applications.

Conclusion

Intrusion Detection Systems (IDS) are essential tools in defending against potential network or system intrusions.

Host-based and network-based IDS serve different purposes, while IDS sensors, signature-based and anomaly-based detection methods, and traffic analysis techniques contribute to effective intrusion detection.

In some systems, the user interface may equate to a manager, director, or console component.

Deploying IDS requires careful consideration of network topology, asset sensitivity, and proper alert management.

Regular monitoring, log analysis, and updates are vital to maintaining an effective IDS system.


Thank You