Intrusion detection System and intrusion prevention system

Presented by :

Deema Alshehri

Layan kandil

Maryam Alotaibi

Outline

- Introduction
- What are IDS and IPS?
- Key Components of IDS and IPS
- Types of IPS
- Detection Methods used by IDS
- Prevention Techniques used by IPS
- Advantages and Limitations of IDS/IPS
- Comparison between IDS and IPS
- Firewall vs. Intrusion Detection System
- Real-World Examples
- How the C|ND Certification Can Help With IDS/IPS
- Conclusion

Introduction

In today's interconnected world, keeping networks and systems secure is extremely important due to rising cyber threats. Intrusion Detection and Prevention Systems (IDS/IPS) are crucial tools in defending against unauthorized access and harmful activities.

This presentation aims to provide an understanding of IDS and IPS, including their key components and techniques for detecting and preventing cyber-attacks.

Intrusion Detection Systems (IDS)

Intrusion Detection Systems (IDS) are security tools that monitor network or host activities to identify and alert against potential intrusions or malicious activities.

IDS Role:

-They are responsible for detecting and alerting about suspicious activities and potential threats.

-They provide early warning signs to administrators or security personnel, allowing for prompt response and mitigation.

Key Components of IDS

- **Sensors/Agents**

  Collect data from network traffic or system logs.

- **Analysis Engine**

  Analyzes collected data to identify potential intrusions.

- **Alerting System**

  Notifies administrators or security personnel about detected threats.

- **Centralized Console**

  Provides a centralized interface for managing and monitoring the IDS

Detection Methods Used by IDS

1- **Signature-based Detection:**

- Compares network traffic against known attack patterns (signatures).
- Effective for detecting well-known and previously identified attacks.

2- **Anomaly-based Detection:**

- establishes a baseline of normal behavior and detects deviations from that baseline
- Useful for detecting unknown attacks that don't match predefined signatures.

3- Behavior-based Detection:

- Monitors the behavior of users and systems to identify suspicious activities.
- Helps in detecting abnormal patterns that may indicate unauthorized access or malicious actions.

Advantages and Limitations of IDS

Advantages:

- Early detection of intrusions
- Improved visibility into network and system activities
- Ability to detect new and unknown threats based on behavioral analysis.

Limitations:

- False positives and False negatives
- Inability to prevent attacks

Intrusion Prevention System (IPS)

is a security tool or device that works in conjunction with an Intrusion Detection System (IDS) a network security technology that monitors network traffic for potential security risks or malicious activity

- It serves as an additional layer of defense to protect networks from unauthorized access, attacks, and exploits.

Key Components of IPS

-Sensors/Agents

Monitor network traffic or system activities for potential threats.

- Enforcement Points

Implement preventive measures, such as blocking or filtering malicious traffic.

- Centralized Management System

Provides centralized control and configuration of IPS policies.

Types of IPS

1. Network-based intrusion prevention system (NIPS)

placed at key network locations, where it monitors traffic and scans for cyber threats

2. Wireless intrusion prevention system (WIPS)

monitor Wi-Fi networks, and remove unauthorized devices

3. Host-based intrusion prevention system (HIPS)

Installed on endpoints, monitor inbound and outbound traffic from that device only

4. Network behavior analysis (NBA)

detect flows that might be associated with DDoS attacks

Prevention Techniques Used by IPS

- Packet Filtering:

packets and block those matching rules, effective for blocking traffic based on criteria like IP addresses or ports.

- Intrusion Signature Matching:

compares network traffic against attack signatures, while protocol anomaly detection identifies and blocks abnormal behavior.

Advantages and Limitations of IPS

Advantages:

- Real-time prevention of attacks
- Blocking of malicious traffic
- Enhanced network and system security

Limitations:

- Performance impact on network.
- Possibility of false positives

Comparison between IDS and IPS

IDS:

- Focuses on detection and monitoring
- provide visibility into network traffic

IPS:

- Focuses on prevention and mitigation.
- Can inspect network packets in real time and take immediate action to block or modify them if they are suspicious

Both systems are placed after the firewall in a network, as it allows them to monitor and analyze traffic, and generate alerts when suspicious activity or a potential attack is detected.

Firewall vs. Intrusion Detection System

- **Firewall:** Filters traffic, ensuring network security.
  - Analyzes packet metadata
  - Allows/blocks traffic based on rules
  - Creates a protective barrier
  - Focuses on inbound/outbound filtering

- **IDS:** Monitors for threats, alerts for timely response
  - Monitors network for threats
  - Real-time alerts to analysts
  - Swift investigation and response
  - Emphasizes detection and alerting

Real-World Examples

1- Snort IDS

Description: Widely used open-source IDS with signature-based detection.

Benefits: Effectively detects and prevents network scanning, malware infections, and unauthorized access attempts.

2- Cisco Firepower IPS

Description: Popular IPS solution with advanced detection techniques.

Benefits: Blocks sophisticated attacks like zero-day exploits and advanced persistent threats (APTs) using real-time threat intelligence.

How the C|ND Certification Can Help With IDS/IPS

The C|ND (Certified Network Defender) is a program that teaches students how to predict, detect, and respond to cyber threats.

The C|ND course is the only certification 100% focused on network security and defense of digital assets.

With the C|ND, you will get an understanding and use of IDS/IPS technologies.

Conclusion

•In conclusion, intrusion detection and prevention systems are essential security measures for protecting networks and systems from unauthorized access and malicious activities.

•By implementing robust IDS and IPS solutions, organizations can maintain the confidentiality, integrity, and availability of sensitive data and critical resources.

References

[1] B. Lutkevich, “What is an intrusion detection system (IDS)? Definition from SearchSecurity,” TechTarget, Oct. 2021. https://www.techtarget.com/searchsecurity/definition/intrusion-detection-system (accessed Feb. 22, 2024).

[2] Fortinet, “What is an Intrusion Detection System (IDS)?,” Fortinet, 2023. https://www.fortinet.com/resources/cyberglossary/intrusion-detection-system (accessed Feb. 23, 2024).

[3] “What Does Intrusion Detection Mean?,” Bizmanualz. https://www.bizmanualz.com/library/what-does-intrusion-detection-mean (accessed Feb. 22, 2024).

[4] What is an Intrusion Prevention System (IPS)? | IBM. (n.d.). https://www.ibm.com/topics/intrusion-prevention-system (accessed Feb. 23, 2024).

[5] What is Intrusion Prevention System*?* / VMware Glossary. (2023, August 9). VMware. https://www.vmware.com/topics/glossary/content/intrusion-prevention-system.html (accessed Feb. 23, 2024).

[6] Jayaraman, N. (2023, December 15). IDS and IPS: Understanding Similarities and Differences. Cybersecurity Exchange. https://www.eccouncil.org/cybersecurity-exchange/network-security/ids-and-ips-differences/ (accessed Feb. 23, 2024).


Thank you!