Intrusion Detection System(IDS) Implementation with Suricata

Project Overview

This project involved designing and implementing an intrusion Detection System (IDS) using Suricata on a Kali Linux virtual machine. The primary goal was to monitor network traffic and detect Malicious activities, thereby enhancing the security posture of a network.

Objectives

- Set up Suricata to monitor network traffic in a defined range (HOME_NET_)]
- Detect and log various types of attacks, including port scans and denial-of-service (DoS) attacks
- Analyze network traffic using Wireshark to understand attack patterns and system responses.

Methodology

Environment Setup

- Installed Suricata on Kali Linux and configured it to monitor traffic.

Monitoring and analysis

- Observed real-time traffic and alerts generated by Suricata
- Analyzed the log files (eve.json, Suricata.log) for insights into detected events.
- Used Wireshark to capture and review network packets during the testing phase

Reporting

- Compiled data and findings into a structured format for review and documentation
- Prepared insights for presentation and further analysis.

Results

- Successfully configured Suricata to detect various attack patterns.
- Generated logs that detailed detected events, which were crucial for analyzing the effectiveness of the IDS
- Enhanced understanding of network security and the importance of real-time monitoring

Conclusion

The project demonstrated the importance of implementing an IDS in network security. Suricata provided valuable insights into potential vulnerabilities and helped establish a proactive security approach.