Overview

This project demonstrates the setup of an Intrusion Detection System (IDS) using pfSense and Snort within the GNS3 environment. The goal is to create a robust network security solution that can monitor and detect potential intrusions in real-time.

Table of Contents

Lab Setup

The lab environment consists of a virtualized setup using GNS3 along with VirtualBox to run the GNS3 VM and pfSense firewall. This configuration allows for flexible network simulation and testing.

Architecture

The architecture includes multiple components, with pfSense acting as the firewall and Snort integrated as the IDS. The system is designed to monitor network traffic and identify suspicious activities.

Initialization

Upon initialization, the system runs smoothly, although it may experience slight delays due to high memory usage, requiring up to 2GB of RAM for optimal performance.

pfSense Configuration

pfSense serves as the core firewall solution in this setup. It includes:

- Basic configurations of pfSense and its interfaces.
- Integration of Snort, which is a widely used IDS that provides a user-friendly interface for setting up detection rules and restrictions.
- Diagnostic tools, such as ping, to verify connectivity within the network.

Key Features:

- Real-time alerts for new entries in the activity log.
- Monitoring capabilities over the LAN interface.

Outcomes

Through this project, we have successfully:

- Setup GNS3 and the GNS3 VM.
- Configured pfSense as a firewall.
- Implemented Snort as an intrusion detection system.
- Monitored LAN traffic effectively, identifying blocked packets and potential threats.

While we can also implement an Intrusion Prevention System (IPS), our current hardware limitations restrict us from performing more complex tasks.

Future Work and Drawbacks

Future improvements could include:

- Enhancing security parameters by adding user authentication and access controls.

Drawbacks:

- Manual assignment of rules to block unwanted sites is required, which can be cumbersome compared to automated solutions available in more advanced firewalls.

Acknowledgments

Thank you for your interest in this project! Your feedback and contributions are welcome as we continue to improve our network security capabilities.