

Snort Network Intrusion Detection System (NIDS)

Overview

This project sets up a basic NIDS system using Snort to detect and alert on suspicious network activities such as ICMP packets.

Setup Process

1. Install dependencies
2. Install DAQ and Snort
3. Create basic directories and configuration
4. Add a sample detection rule
5. Start monitoring the network

Skills Demonstrated

- Linux System Administration
- Network Intrusion Detection
- Security Monitoring
- Rule Writing and Analysis