Wazuh SIEM Lab Report

# Overview

This document outlines the configuration and testing of a Security Information and Event Management (SIEM) system using Wazuh in a home lab environment. This project demonstrates real-world cybersecurity monitoring techniques through the integration of various servers and a vulnerable virtual machine.

# Environment Setup

The lab environment consists of several virtual machines (VMs):  
- Ubuntu Server (Wazuh Manager + Dashboard + Indexer)  
- Ubuntu Server (DNS and DHCP services)  
- Kali Linux (attacker machine)  
- Metasploitable2 (target system)

# Wazuh Configuration

Wazuh was deployed on a dedicated Ubuntu Server. Configuration included:  
- Setting up Wazuh indexer, manager, and dashboard.  
- Configuring network connectivity (Internal Network) for isolated communication.  
- Installing Wazuh agents on:  
 - DNS/DHCP server  
 - Kali Linux (attacker system)  
 - Metasploitable2 (target system)  
- Fixing agent issues with proper permissions and service dependencies.  
- Ensuring correct server IP addresses were configured on the agents.

# Attack Simulation

The Kali Linux VM was used to simulate various attacks on the Metasploitable2 system including:  
- Port scanning (Nmap)  
- Enumeration  
- Exploits via Metasploit Framework  
  
Wazuh monitored these activities and logged alerts under the Security Events section of the dashboard.

# Observations

Using the Wazuh dashboard, events related to the attacks were logged and categorized. The alerts demonstrated that Wazuh effectively monitored the security of all connected agents, highlighting key suspicious activity such as login attempts, shell usage, and vulnerabilities.

# Conclusion

This project demonstrates the viability of setting up a home SIEM lab using Wazuh. The knowledge gained from configuring the system and interpreting logs is valuable for entry-level cybersecurity analysts or those studying for certifications like CompTIA Security+ or Wazuh Fundamentals.