WAZUH Home Lab – SIEM and File Integrity Monitoring

Overview

Wazuh is a free, open-source security platform that provides:
- Log analysis
- File integrity monitoring
- Intrusion detection
- Vulnerability detection
- Real-time alerting

This guide explains how to set up a basic Wazuh lab for learning and experimentation.

Lab Architecture

Components:
- Wazuh Manager (Kali Linux): Collects, analyzes, and stores security data.
- Wazuh Agent (Windows Host): Sends logs and system events to the manager.

Network Configuration: Both systems must be on the same network.

Prerequisites

- Kali Linux installed
- Internet access on Kali
- Administrative access on Windows host
- Basic Linux knowledge (recommended)

Installing Wazuh Manager (Kali Linux)

Step 1: Add Wazuh GPG Key
https://packages.wazuh.com/key/GPG-KEY-WAZUH
Command:
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | sudo gpg --dearmor -o /usr/share/keyrings/wazuh-archive-keyring.gpg

Step 2: Install Wazuh
https://packages.wazuh.com/4.12/wazuh-install.sh
Command:
curl -sO https://packages.wazuh.com/4.12/wazuh-install.sh && sudo bash ./wazuh-install.sh -a -i

Accessing Wazuh Dashboard

Find Kali IP:
ifconfig

Open browser:

https://<KALI-IP>

Login using credentials shown after installation.

Installing Wazuh Agent (Windows)

Download link:
https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package-windows.html

Install using default settings.

Registering Agent

Generate agent key:
sudo /var/ossec/bin/manage_agents

Steps:
- Press A to add agent
- Assign name
- Extract key (E)

Paste key in Windows Agent Manager and restart service.

File Integrity Monitoring (Windows)

Edit config:
C:\Program Files (x86)\ossec-agent\ossec.conf

Add:
<directories realtime="yes">C:\Users\abc\Test</directories>

Restart agent service.

Verification

Check Dashboard → Agents → Status Active
Modify files in monitored folder
Confirm alerts in Integrity Monitoring section.