Wazuh SIEM & File Integrity Monitoring Lab

A Home-Lab Implementation of Enterprise Endpoint Security Monitoring

By Neemkar Sai Pratheek

B.Tech in Computer Science and Engineering (Specialization in Cybersecurity)

VIT Bhopal University

Introduction

Due to the escalating incidence of malware, ransomware, and insider threats, numerous organizations rely significantly on Security Information and Event Management (SIEM) systems to monitor endpoints and detect suspicious activity in real time.A SIEM collects logs, system events, and security telemetry from multiple devices and provides centralized visibility to security teams.

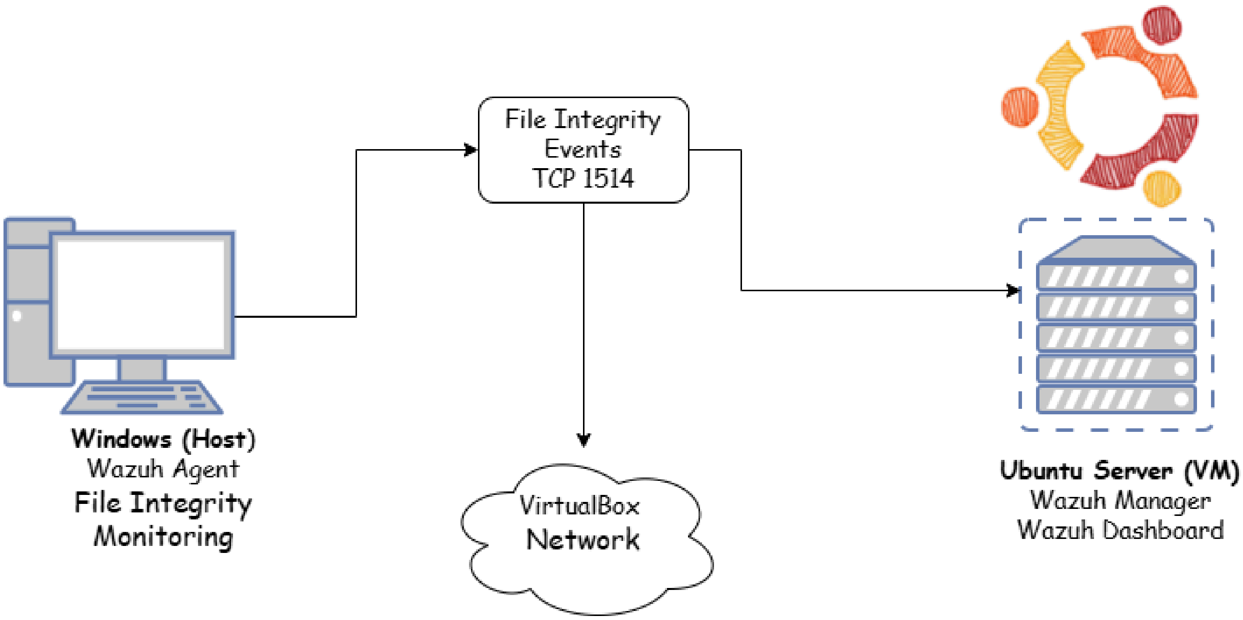
The objective of this project is to deploy a real-world SIEM solution using Wazuh to monitor a Windows endpoint from a Linux-based security server and detect unauthorized file changes, hidden files, and cryptographic integrity violations.

What is Wazuh?

Wazuh is a free, open-source security monitoring solution that unifies Extended Detection and Response (XDR) and Security Information and Event Management (SIEM) capabilities. It's designed to protect endpoints and cloud workloads by collecting, aggregating, indexing, and analyzing security data.

Lab Architecture

The lab consists of two systems:



1. A Windows host machine running the Wazuh Agent
2. An Ubuntu virtual machine running the Wazuh Manager and Dashboard

Both systems are connected using a VirtualBox host-only network, allowing secure communication between the agent and the SIEM server.

Wazuh Deployment:

The Wazuh Manager was installed on Ubuntu using the official Wazuh installation script. This installed the Wazuh Manager, Indexer, and Dashboard.

The Wazuh Dashboard provides a web-based interface to view security alerts, agent status, and integrity monitoring results.The official Wazuh installation script was used to deploy the Wazuh Manager on an Ubuntu system. This single installation process set up the Wazuh Manager, the Indexer, and the Dashboard.

The Wazuh Dashboard is a web interface that offers visualizations of security alerts, the status of monitored agents, and the results from integrity monitoring.

Windows Agent Installation & Onboarding:

The Wazuh Agent was installed on the Windows host. The agent was registered with the Ubuntu manager using a secure key generated on the Wazuh Manager. After registration, the Windows system appeared as an active agent in the SIEM dashboard, confirming secure communication.Following the successful installation and registration of the Wazuh agent on the Windows host, secure communication was established between the Windows system and the Wazuh Manager (Ubuntu). The agent was registered securely with the Ubuntu manager utilizing a generated key. Consequently, the Windows system was visible as an active agent within the SIEM dashboard.

File Integrity Monitoring (FIM):

File Integrity Monitoring (FIM) detects changes in files and directories to identify malware, unauthorized access, and system tampering.

In this lab, a specific directory on the Windows system was configured in the OSSEC agent configuration file (ossec.conf) for real-time monitoring. The Wazuh agent continuously monitored this directory and sent alerts whenever files were created, modified, deleted, or hidden.

- File Integrity Monitoring (FIM) is used to detect modifications to files and directories, helping to identify potential threats like malware, unauthorized access, and system tampering.
- In this lab exercise, a specific Windows directory was set up for real-time monitoring.
- This monitoring was configured using the OSSEC agent configuration file

(ossec.conf).

- The Wazuh agent continuously watched this directory.
- Alerts were generated by the agent upon any file creation, modification, deletion, or concealment.

Advanced Integrity Checks:

1. Advanced integrity-verification mechanism was implemented to enhance the lab's effectiveness and reliability.
2. These mechanisms include cryptographic hashing algorithms like checksum and SHA-1.
3. Wazuh accurately verifies file authenticity using these measures and hidden file detection to identify stealthy creations.
4. The system detects even the smallest unauthorized modification or file attribute change by comparing cryptographic hashes and file attributes.

Results and Observations:

1. The Windows Wazuh agent remained active and successfully communicated with the Ubuntu SIEM server.
2. File creation, modification, deletion, and hidden file attributes were detected in real time.
3. Alerts were generated and displayed on the Wazuh dashboard for every file system change.
4. Cryptographic hashing (checksum and SHA-1) detected integrity violations through hash mismatches.
5. Hidden files were correctly identified as suspicious activity.
6. The centralized dashboard provided clear visibility into all security events.
7. The lab validated Wazuh’s ability to monitor endpoints and ensure file integrity in real time.

Conclusion

This lab successfully demonstrated the deployment of an enterprise-grade SIEM using Wazuh to monitor a Windows endpoint from a centralized Ubuntu server. Through real-time file integrity monitoring, hidden file detection, and cryptographic hashing, the system was able to detect unauthorized file changes and potential security threats. The results confirmed the effectiveness of Wazuh in providing continuous endpoint visibility and reliable security alerts. Overall, this project provided valuable hands-on experience in SIEM deployment, endpoint security, and Security Operations Center (SOC) practices.