Wazuh SIEM Lab Project

Wazuh SIEM Lab Project Documentation

1. Abstract

This project demonstrates the deployment and testing of a Security Information and Event Management (SIEM) system using Wazuh, an open-source security monitoring platform. The deployment was carried out using a pre-built Wazuh OVA (Open Virtual Appliance) file inside a virtualized environment. The objective was to set up Wazuh quickly, configure agents on monitored endpoints, and test detection capabilities using simulated security events.

2. Objective

• Deploy Wazuh SIEM using a ready-made OVA file on a virtual machine.
• Configure network settings to allow agent–manager communication.
• Install and connect Wazuh agents on endpoints.
• Generate test security events to evaluate detection and alerting.
• Monitor and analyze events using the Wazuh dashboard.

3. Tools & Technologies Used

Title	Title
Tool / Technology	Purpose
Wazuh OVA	Pre-configured Wazuh Manager, OpenSearch, and Dashboard.
VMware Workstation / VirtualBox	Virtualization platform for running the Wazuh VM.
Windows 10 / Linux Endpoints	Systems for Wazuh agent installation.
Wazuh Agent	Installed on endpoints to send logs and events.
Nmap / Kali Linux	For generating test attacks.
Web Browser	For accessing Wazuh dashboard.

4. Lab Setup Architecture

```
+------------------+    +-----------------+   +---------------+
|  Endpoint (Agent | -> |                 |   |               |
|  Windows / Linux |    |                 |   |               |
+------------------+    |                 |   |               |
|  Wazuh Manager   |<-->|   OpenSearch /  |   |               |
+------------------+    |    .OVA VM      |   |   Dashboard   |
|  Endpoint (Agent)| -> |                 |   |               |
+------------------+    +-----------------+   +---------------+
```

5. Implementation Steps

Step 1: Deploy Wazuh OVA

1. Download the official Wazuh OVA file from Wazuh Downloads.
2. Import the OVA into VirtualBox or VMware.
3. Allocate resources (Recommended: 4GB RAM, 2 CPUs, 50GB storage).
4. Configure bridged networking or NAT with port forwarding so the Wazuh VM is accessible from the host and other endpoints.

Step 2: Start Wazuh VM

1. Power on the VM.
2. Login with default credentials provided in Wazuh documentation.
3. Note the IP address of the VM using:

```
ip addr
```

Step 3: Access Wazuh Dashboard

1. Open browser and go to:

```
https://<WAZUH_VM_IP>
```

2. Login using default admin credentials.
3. Change the default password for security.

Step 4: Install Wazuh Agents on Endpoints

• From the dashboard, navigate to Agents → Deploy new agent.
• Select the OS type and follow installation instructions.
For Windows: Download and run the MSI installer, enter Wazuh VM IP.
For Linux: Download and run the shell installer, then start the agent service.

Step 5: Test Detection

• Run port scan from Kali Linux using:

```
nmap -A <agent-ip>
```

• Attempt failed logins.
• Upload suspicious files to trigger malware detection.

6. Results

• Wazuh VM successfully collected logs from agents.
• Dashboard displayed alerts for scanning, brute-force attempts, and file integrity monitoring.
• Visualizations and correlation rules worked as expected.
(Insert screenshots of Wazuh dashboard, alerts, and event logs here)

7. Conclusion

The lab successfully deployed Wazuh SIEM using an OVA file, making setup quick and straightforward. Agents on multiple endpoints reported events in real-time, and security incidents were detected accurately. This method is ideal for testing and learning SIEM functionality without complex installation steps.

8. References

• Wazuh Official Documentation: https://documentation.wazuh.com/
• Wazuh OVA Deployment Guide:
https://documentation.wazuh.com/current/deployment-options/virtual-machine/virtual-machine.html
• MITRE ATT&CK Framework: https://attack.mitre.org/

• Author : Swastik Sagar