## **Wazuh Windows Agent SIEM Lab (Kali Manager)**

This project demonstrates how to configure a Windows 11 machine as a Wazuh agent and connect it to a Kali Linux system running the Wazuh manager. The lab simulates a basic **Security Information and Event Management (SIEM)** setup where Windows endpoint logs are forwarded to and monitored by a centralized Wazuh manager. The lab was completed in a fully offline environment using VirtualBox and Host-Only networking.

## **🧪 Lab Overview**

* **SIEM Platform**: Wazuh (open-source security platform)
* **Wazuh Manager OS**: Kali Linux
* **Agent OS**: Windows 11
* **Wazuh Version**: 4.7.x
* **Network Type**: Host-Only Adapter (VirtualBox)
* **Agent Status**: Connected and Active

## **🛠️ Tools Used**

* VirtualBox
* Kali Linux (Wazuh Manager)
* Windows 11 (Wazuh Agent)
* Wazuh Agent Installer (Windows MSI)
* Command Line (Kali + Windows)

## **🧰 Step-by-Step Setup**

### **1. Prepare VirtualBox Network**

* Both VMs were attached to **Host-Only Adapter**
* Assigned static IPs:
  + **Kali (Manager)**: 192.168.56.11
  + **Windows (Agent)**: 192.168.56.10

📷 *Insert screenshot of both VM network settings here*

### **2. Install Wazuh Manager on Kali**

Since Kali is unsupported by default, we bypassed the system check:

curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh  
sudo bash wazuh-install.sh -i

If needed (due to unsupported OS warning):

sudo bash wazuh-install.sh --ignore-check

📷 *Insert screenshot of successful installation or Wazuh services running here*

### **3. Verify Required Ports Are Open**

sudo ufw allow 1514/tcp  
sudo ufw allow 1515/tcp  
sudo ufw enable

Check listening ports:

sudo ss -tuln | grep 151

Expected output:

tcp 0 0 0.0.0.0:1514 0.0.0.0:\* LISTEN  
...   
tcp 0 0 0.0.0.0:1515 0.0.0.0:\* LISTEN

📷 *Insert screenshot of ufw rules or* ***ss -tuln*** *output here*

### **4. Generate Wazuh Agent Auth Key**

sudo /var/ossec/bin/manage\_agents

* Press A to add agent
* Enter name (e.g., win-lab) and IP
* Copy the generated key for use on Windows

📷 *Insert screenshot of key generation here*

### **5. Assign Kali IP Manually**

sudo ip addr add 192.168.56.11/24 dev eth0  
sudo ip link set eth0 up

Confirm:

ip a | grep 192

📷 *Insert screenshot of Kali IP confirmation*

### **6. Install Wazuh Agent on Windows 11**

* Transferred .msi file manually
* Ran installer
* Opened **Wazuh Agent Manager**
  + Entered **Manager IP**: 192.168.56.11
  + Pasted **auth key**
  + Clicked **Save**, then **Manage > Start Agent**

📷 *Insert screenshot of Agent Manager GUI with fields filled*

### **7. Confirm Agent Connection**

On Kali:

sudo /var/ossec/bin/agent\_control -l

Expected output:

ID: 002, Name: DESKTOP-XXXXX, IP: any, Active

📷 *Insert screenshot of connected agent list*

Optional: Tail the Wazuh log to see connection in real-time:

sudo tail -f /var/ossec/logs/ossec.log

## **✅ Results**

* Agent successfully registered and shown as **Active** in manager
* TCP traffic on port 1514 confirmed from agent to manager
* Simulated SIEM behavior by centralizing Windows endpoint logs
* Fully functioning offline Wazuh SIEM lab with proof of concept

## **📸 Screenshots to Include**

Put all images into a screenshots/ folder. Reference them in the README as shown above:

* VM network adapter settings
* IP confirmation
* Wazuh manager ports
* Agent key generation
* Wazuh Agent GUI (Windows)
* Agent status on Kali

## **📦 Repo Suggestions**

* Repo name: wazuh-windows-agent-siem-lab
* .gitignore: include \*.iso, \*.ova, \*.vdi, etc.
* Keep your README.md, screenshots/, and any relevant configs

## **🙌 Credits**

Built and tested by [Your Name], a cybersecurity grad student using Kali Linux and Windows 11 on VirtualBox to simulate real-world endpoint monitoring with a basic open-source SIEM.

Feel free to fork or use this as a base for blue team, SOC, or SIEM demos.