Security Lab Architecture and Setup

Virtualized Security Lab Environment for Threat Simulation and Detection

Report by: Wayne Howlett

April 2026

Version 1.0

1. Project Title

Virtualized Security Lab Environment for Threat Simulation and Detection
Environment Type: Virtualized Security Lab
Primary Focus: Threat Detection & Analysis
Core Tools: Wazuh, Sysmon, Kali Linux
Key Capabilities: Logging, Detection, Simulation

---

2. Objective

This project aims to design and implement a centralized virtualized security lab environment for the simulation, detection, and analysis of cybersecurity threats. The environment is intended to support hands-on learning, portfolio development, and practical experience in security operations and security engineering.

---

3. Purpose

This lab provides a controlled environment in which to:

- Simulate real-world cyberattacks.
- Capture and analyze logs from multiple systems.
- Implement and validate detection mechanisms.
- Practice incident response procedures.
- Support the development of structured security documentation.

---

4. Scope

The lab environment includes the following components:

- A centralized Security Information and Event Management (SIEM) platform using Wazuh.
- Multiple virtual machines representing endpoints and infrastructure systems.
- A designated attacker system for generating realistic threat activity.
- A private internal network to enable secure communication among lab assets.

The environment will be used to conduct and evaluate multiple security scenarios, including:

- Brute-force attacks.
- Phishing simulations.
- Malware activity analysis.
- Web application attack testing.
- System hardening validation.

---

5. Architecture Overview

5.1 Core Components

The lab consists of the following systems:

- **Wazuh SIEM Server:** Centralized platform for log collection, alerting, and security monitoring.
- **Linux Server:** Simulated infrastructure host providing services such as SSH and web hosting.
- **Windows Endpoint:** Simulated user workstation configured for endpoint telemetry collection.
- **Kali Linux Attacker:** Adversary simulation system used to generate attack scenarios.

5.2 Network Design

All virtual machines are connected through an isolated internal network to ensure controlled and secure interaction between systems.

Network Configuration

- **Network type:** Internal Network (lab-net)
- **Communication:** Permitted between all systems within the lab
- **External exposure:** None

IP Addressing Scheme

System	IP Address
Wazuh SIEM	192.168.100.10
Linux Server	192.168.100.20

System	IP Address
Windows Endpoint	192.168.100.30
Kali Attacker	192.168.100.40

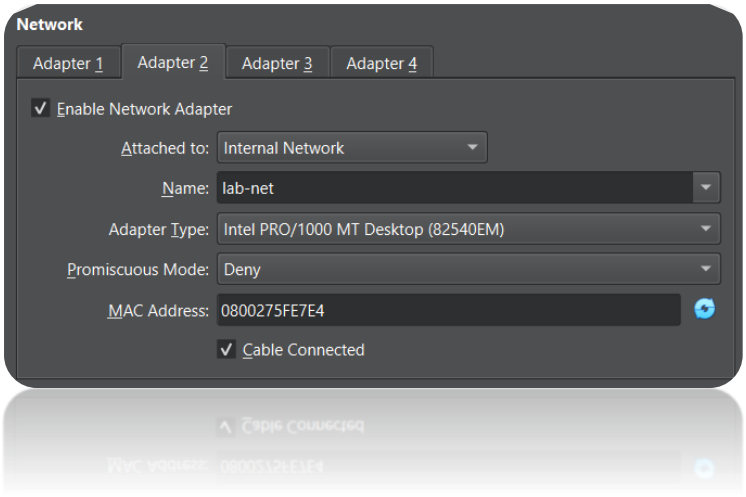

Figure 1. Virtual machine network configuration showing the isolated internal lab network.

---

6. Environment Setup

6.1 Virtualization Platform

The lab is hosted on VirtualBox, or an equivalent hypervisor, with the required extension pack installed.

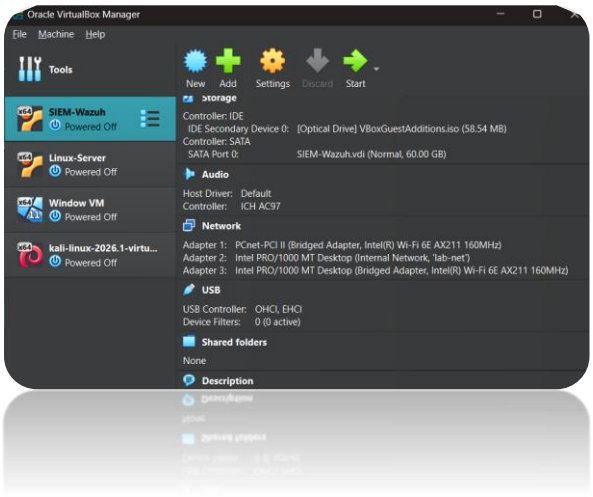

Figure 2. VirtualBox host environment prepared for deployment of the security lab.

6.2 Virtual Machine Specifications

6.2.1 Wazuh SIEM Server

- **Operating system:** Ubuntu Server
- **Memory:** 4-6 GB RAM
- **Storage:** 50 GB
- **Role:** Centralized log aggregation, detection, and analysis

Figure 3. Wazuh SIEM virtual machine configuration and resource allocation.

6.2.2 Linux Server

- **Operating system:** Ubuntu Server
- **Memory:** 2 GB RAM
- **Storage:** 20-30 GB
- **Services:**
    - SSH for remote access simulation
    - Nginx for web service and log generation

Figure 4. Linux server virtual machine configuration and enabled services.

6.2.3 Windows Endpoint

- **Operating system:** Windows 10 or Windows 11
- **Memory:** 4 GB RAM
- **Storage:** 50 GB
- **Tools:**
    - Sysmon for enhanced endpoint logging

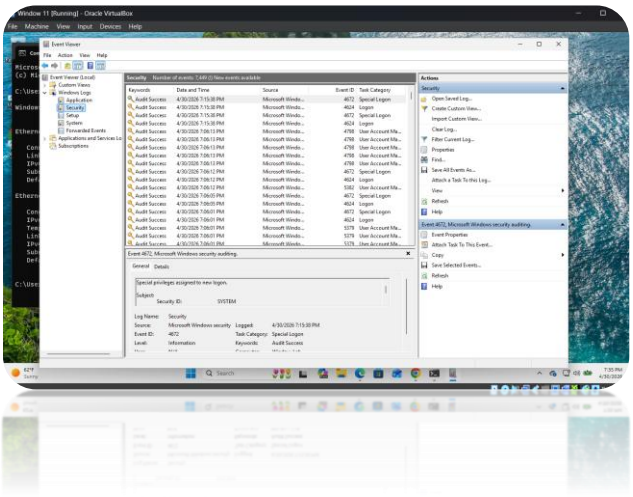

Figure 5. Windows endpoint configuration with telemetry tooling installed.

6.2.4 Kali Linux Attacker

- **Operating system:** Kali Linux
- **Memory:** 2-4 GB RAM
- **Tools:**

- Nmap
- Hydra
- Additional penetration testing utilities

Figure 6. Kali Linux attacker system prepared for threat simulation activities.

---

7. SIEM Deployment

Wazuh is deployed on the Ubuntu-based SIEM server to provide centralized logging, event analysis, and detection capabilities. Wazuh architecture is built around agents that forward endpoint data to central components for analysis, storage, and visualization, and its all-in-one model is commonly suited to lab or small-scale environments.

7.1 Installation Overview

```
sudo apt update && sudo apt upgrade -y
curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh
sudo bash wazuh-install.sh -a
```

7.2 Post-Installation Validation

- Verify that Wazuh services are running correctly.
- Access the Wazuh dashboard through a web browser.
- Confirm overall system health and service availability.

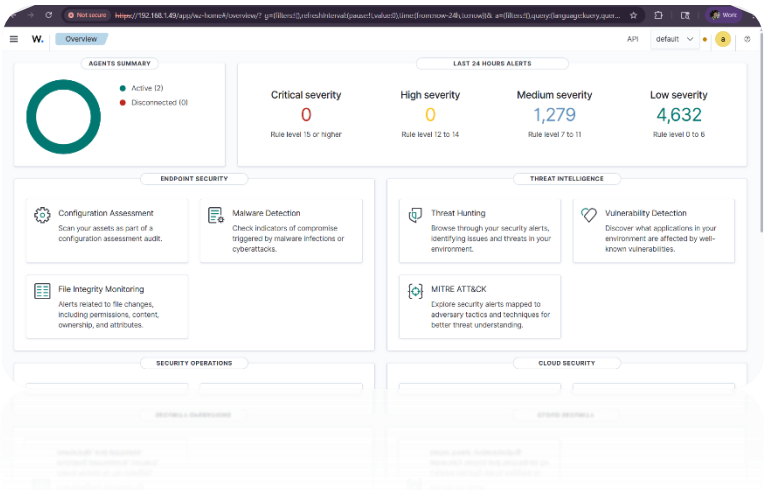

Figure 7. Wazuh dashboard following successful installation and initial access.

---

8. Agent Configuration

8.1 Linux Agent

The Linux agent is installed on the Linux server to forward:

- Authentication logs
- System logs

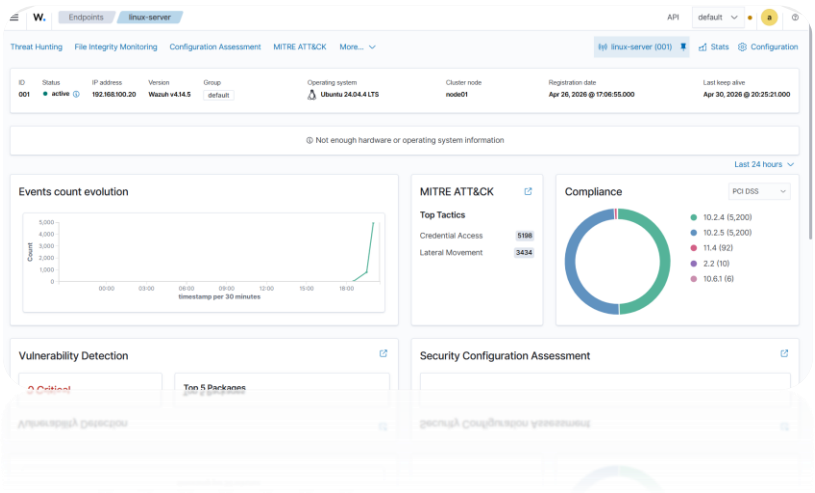

Figure 8. Linux endpoint successfully registered as an active Wazuh agent.

8.2 Windows Agent

The Windows agent is installed on the Windows endpoint to collect:

- Windows Event Logs
- Sysmon telemetry

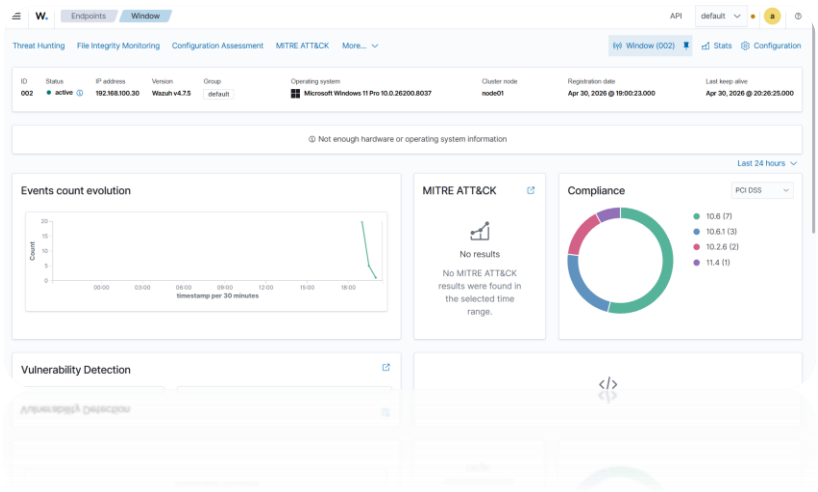

Figure 9. Windows endpoint successfully registered with Sysmon telemetry enabled.

8.3 Verification

Successful agent configuration is confirmed when:

- Endpoints appear in the Wazuh dashboard.
- Logs are actively ingested by the SIEM platform.

---

9. Validation Testing

The following tests are performed to verify the environment is functioning as intended:

9.1 Connectivity Testing

All lab systems successfully communicate across the internal network.

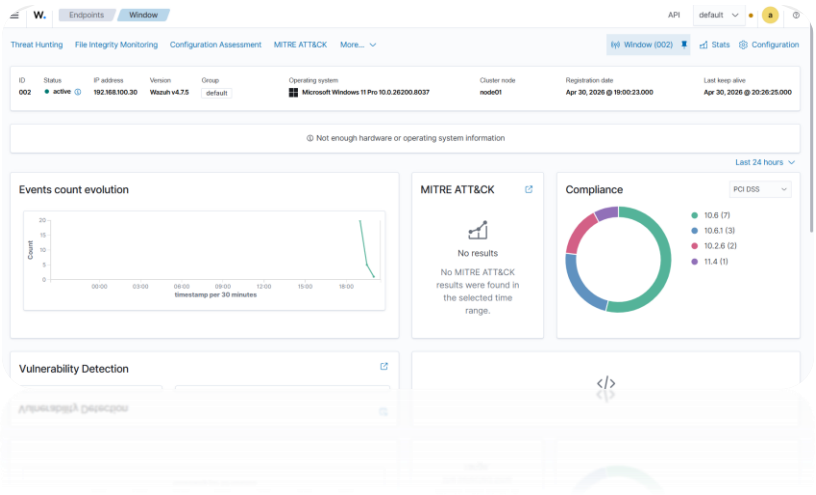

Figure 10. Connectivity validation between lab systems across the internal network.

9.2 Log Ingestion Testing

- Restarting services on the Linux server generates relevant system logs.
- User or system activity on the Windows endpoint generates event logs.
- The resulting logs are visible in Wazuh.

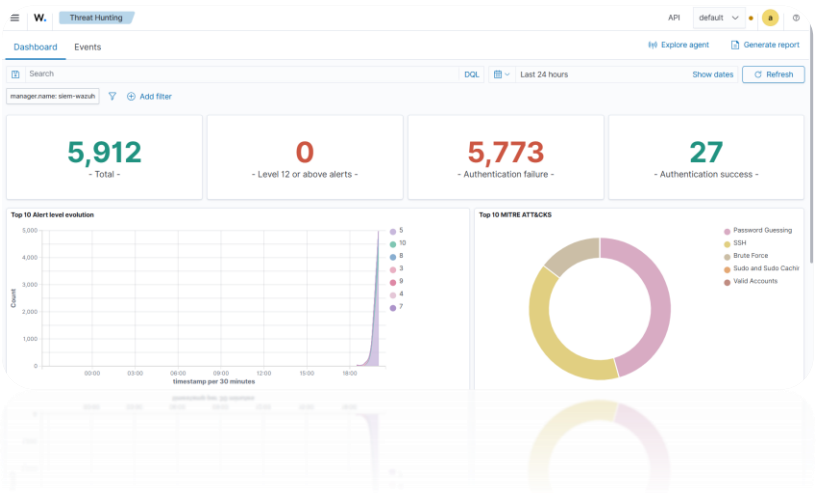

Figure 11. Example log ingestion events displayed within the Wazuh platform.

---

10. Initial Threat Simulation

An initial brute-force attack is conducted from the Kali Linux system to validate detection and logging workflows.

10.1 Example Command

hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://192.168.100.20

10.2 Expected Results

Expected Results:

- Multiple failed SSH login attempts recorded in /var/log/auth.log
- Events ingested and normalized within Wazuh
- Correlated alerts triggered based on brute-force behavior
- Source IP of attacker identified through log analysis

The source IP address (192.168.100.40) corresponding to the Kali Linux attacker system was successfully identified within the Wazuh alert data.

Figure 12 (Appendix A7) Brute-force simulation executed from the Kali Linux attacker system.

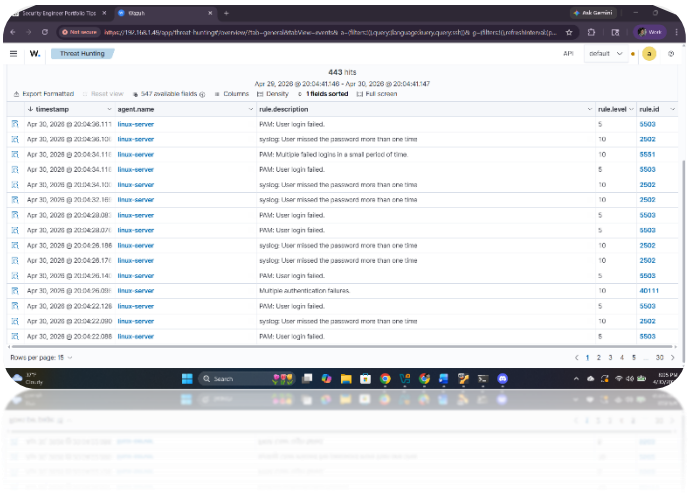

Figure 13. Resulting authentication failures and related alert activity visible in Wazuh.

---

11. Evidence Collection

The following artifacts are collected during setup and validation activities:

- Virtual machine configuration details
- Network configuration screenshots
- Wazuh dashboard screenshots
- Relevant log entries and alerts
- Attack command output and supporting test evidence

---

12. Planned Use Cases

This lab environment will support:

- Individual security project development
- Detection engineering exercises
- Incident response simulations
- Vulnerability assessment activities
- Professional portfolio demonstration

---

13. Conclusion

The virtualized security lab provides a scalable and controlled environment for simulating realistic cybersecurity scenarios. It supports hands-on experience in threat detection, log analysis, and incident response, while also serving as a foundation for structured, evidence-based security portfolio projects.

Appendix A. Build Screenshots and Supporting Evidence

Appendix A provides supporting screenshots and evidence captured during the setup, validation, and attack simulation phases of the lab. Each artifact corresponds to specific figures referenced throughout the report.

- Figure 1 → A1_virtualbox_network.png
- Figure 2 → A2_wazuh_install_output.png
- Figure 3 → A3_wazuh_vm_config.png
- Figure 4 → A4_linux_server_config.png
- Figure 5 → A5_windows_endpoint_sysmon.png
- Figure 6 → A6_kali_tools_ready.png
- Figure 7 → A10_wazuh_dashboard_summary.png
- Figure 8 → A3_linux_agent_install.png
- Figure 9 → A4_windows_agent_install.png
- Figure 10 → A10_connectivity_validation.png
- Figure 11 → A11_log_ingestion.png
- Figure 12 → A7_hydra_attack.png
- Figure 13 → A13_detection_drilldown.png