Wazuh SIEM Project Report

1. Introduction

This project demonstrates the deployment and use of the Wazuh Security Information and Event Management (SIEM) platform to monitor and analyze Windows authentication events. The primary focus of this project is to collect, visualize, and investigate Windows Security Event Logs, specifically failed logon attempts (Event ID 4625), in a controlled lab environment.

The goal of this project is to simulate a real-world SOC (Security Operations Center) scenario where security analysts monitor endpoint activity, detect suspicious authentication behavior, and perform basic investigation using SIEM tools.

---

2. Project Objectives

The main objectives of this project are:

- Deploy a Wazuh all-in-one server using a prebuilt OVA image
- Install and configure a Wazuh agent on a Windows endpoint
- Verify successful agent enrollment and communication
- Collect Windows Security Event Logs
- Analyze failed authentication attempts using Wazuh Discover
- Document findings in a professional SOC-style report

---

3. Environment Setup

3.1 Virtual Environment

The project was implemented using a virtualized lab environment consisting of:

- **Wazuh Server:** Deployed using the official Wazuh OVA (all-in-one stack)
- **Windows Endpoint:** Microsoft Windows 10 Pro (virtual machine)
- **Hypervisor:** VirtualBox Both virtual machines were configured on the same internal network to allow secure communication between the Wazuh server and the Windows agent.

4. Wazuh Deployment

4.1 Wazuh Server Installation

The Wazuh server was deployed using the official OVA image. This installation includes:

- Wazuh Manager
- Wazuh Indexer
- Wazuh Dashboard

After deployment, the Wazuh Dashboard was accessed via a web browser using the server IP address.

4.2 Windows Agent Installation

The Wazuh agent was installed on the Windows 10 virtual machine using the official Wazuh agent installer. After installation:

- The agent was configured to connect to the Wazuh server
- The agent service was started successfully
- The endpoint appeared as **Active** in the Wazuh Dashboard

---

5. Agent Verification

Agent connectivity and health were verified through the Wazuh Dashboard:

- The Windows endpoint appeared under **Agents Management**
- Agent status showed **Active**
- Operating system and agent version information were correctly displayed

This confirmed successful enrollment and communication between the agent and the server.

---

6. Log Collection

The Windows agent was configured to collect Windows Security Event Logs. These logs include authentication-related events such as:

- Successful logons
- Failed logon attempts
- System and service-related authentication activity

Collected logs were forwarded to the Wazuh server and indexed for analysis.

---

7. Event Analysis

7.1 Focused Event

This project focused on analyzing **Windows Security Event ID 4625**, which represents a failed logon attempt.

7.2 Query Used

The following query was used in the Wazuh Discover interface to identify failed authentication events:

data.win.system.eventID: 4625

7.3 Analysis Details

The collected events provided detailed information, including:

- Target username
- Source IP address
- Authentication package
- Logon process name
- Timestamp of the event

These details are essential for identifying suspicious login behavior such as brute-force attempts or unauthorized access attempts.

---

8. Findings

Based on the analysis, the following findings were observed:

- The Windows agent was successfully deployed and remained active
- Windows Security Event Logs were collected without errors
- Failed logon attempts (Event ID 4625) were successfully detected
- Authentication data was clearly visible and suitable for investigation

This confirms that Wazuh is effectively monitoring Windows authentication activity.

---

9. Security Value

This project demonstrates how Wazuh can be used in a SOC environment to:

- Monitor endpoint authentication behavior
- Detect failed login attempts
- Support incident investigation and threat detection
- Improve visibility into endpoint security events

---

10. Conclusion

This project successfully demonstrated the deployment and use of Wazuh for monitoring Windows authentication events. By integrating a Windows endpoint with the Wazuh SIEM platform, security-relevant logs were collected, analyzed, and investigated effectively.

The project reflects practical SOC-level skills, including SIEM deployment, log analysis, and security event investigation, and provides a solid foundation for more advanced threat detection and incident response use cases.

---

11. Future Improvements

Potential future enhancements for this project include:

- Simulating brute-force attacks for advanced detection
- Creating custom Wazuh rules
- Implementing alerting and notifications
- Expanding monitoring to additional endpoints
- Integrating threat intelligence feeds
