Home Lab SOC Simulation Report

Generated on: July 23, 2025

Project Overview

This project simulates a real-world SOC scenario where a Windows endpoint is monitored using Wazuh SIEM. The goal is to detect and analyze simulated malicious activities through system logs and alerts.

Environment Setup

- Wazuh Manager: Ubuntu VM (VirtualBox)
- Endpoint Agent: Windows VM with Wazuh Agent and Sysmon installed
- Agent successfully registered and connected to the manager

Attack Simulation

A Python script (malware_sim.py) mimicked malware behavior by:

1. Writing a registry key for persistence
2. Creating a scheduled task to run calc.exe every 5 minutes
3. Executing suspicious processes (cmd.exe, PowerShell, calc.exe)

Detected Activities

The following MITRE ATT&CK techniques were triggered and logged:

- T1059.001: PowerShell command execution
- T1078: Valid user logon success
- T1087: Account discovery via net.exe
- T1105: Command and control
- T1547: Registry run key & scheduled task persistence

Wazuh successfully generated alerts with relevant rule IDs and log entries.

Outcome

- Wazuh Agent registration issues resolved (duplicate agent name)
- Real-time detection confirmed for all simulated behaviors

- Logs verified through ossec.log and Wazuh Dashboard
- Alert rules, tactics, and techniques properly mapped

This confirms the home lab setup is working as intended for SOC simulations.

Next Steps

Proceed to the next cybersecurity project:

- Vulnerability Management Workflow (OpenVAS/Nessus + OWASP Juice Shop)
- Optional: Publish this report and logs to GitHub portfolio