Home Lab SOC Simulation Report

Generated on: July 23, 2025

Project Overview

This report was prepared by Aino Astillero to document a simulated SOC scenario in a home lab environment. The objective was to test the ability to detect and analyze suspicious behavior on a monitored endpoint using Wazuh SIEM.

Environment Setup

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

Attack Simulation

A custom Python script (`malware_sim.py`) was executed to simulate malware-like behavior:

1. Created a registry key under HKCU\...\Run to launch calc.exe at login.
2. Scheduled a Windows task to execute calc.exe every 5 minutes.
3. Launched calc.exe via cmd.exe and PowerShell.

The intent was to generate realistic endpoint activity that can be detected and logged by Wazuh.

Detected Activities

Wazuh generated multiple alerts during the simulation, each mapped to MITRE ATT&CK techniques, including:

- T1059.001: PowerShell command execution
- T1078: Valid account logon
- T1087: Account discovery via net.exe
- T1105: Command and Control (script file creation)
- T1547: Persistence via registry key and scheduled task

Alert logs were verified using both the Wazuh Dashboard and `ossec.log`.

Incident Response

While Wazuh is primarily a detection tool, initial incident response was conducted manually:

- Confirmed alert generation in real time
- Manually terminated recurring calc.exe processes triggered by the scheduled task
- Disabled or deleted the malicious registry key and scheduled task used for persistence

Outcome

- Successful detection of all simulated behaviors
- Validation of Sysmon-Wazuh integration
- Agent communication re-established after IP change (handled manually)
- Demonstrated effectiveness of Wazuh SIEM in detecting endpoint-based threats in a home lab setup

Next Steps

The next phase will focus on vulnerability management using tools like OpenVAS or Nessus in conjunction with vulnerable web apps (e.g., OWASP Juice Shop). This report, along with supporting logs and artifacts, will be published on GitHub as part of a cybersecurity portfolio.