Security Detection Lab Report

Name: Mustafa Abbasi
Date: September 2025
Project: Home SOC Lab using Wazuh SIEM

The purpose of this project was to build a home Security Operations Center (SOC) environment and test how well custom rules in Wazuh SIEM can detect common attack techniques. I set up three virtual machines: one running the Wazuh Manager, one as the target with the Wazuh agent installed, and one attacker system to simulate malicious activity. The goal was to simulate real-world attacks, create detection rules, and validate that alerts were triggered as expected.

Methodology

I focused on three main types of attacks:

1. **SSH Brute Force**
    - Used Hydra to generate repeated failed login attempts.
    - Wazuh was configured with a custom correlation rule to trigger after six failed SSH logins from the same IP within two minutes.
2. **Apache Web Scan**
    - Ran Nmap scans to hit open web ports and generate a large number of 400/501 HTTP errors.
    - Wazuh rules correlated multiple Apache error events in a short timeframe to identify possible web reconnaissance.
3. **Privilege Escalation Attempts**
    - On the target VM, I deliberately entered incorrect sudo passwords multiple times and then attempted successful escalations.
    - Custom rules were written to detect both repeated sudo failures and login failures, and another correlation rule tied them together to highlight a potential escalation attempt.

For each scenario, I captured alerts and logs in Wazuh, created hero screenshots, and organized evidence into folders for easy review.

Results

- **SSH Brute Force:** Alerts fired correctly after six failed attempts from the attacker IP. The rule successfully tracked repeated failures and flagged the brute force attempt.

- **Apache Scan:** Multiple error responses were correlated within the set timeframe, generating alerts that aligned with simulated scanning activity.

- **Privilege Escalation:** Rules triggered on repeated sudo failures, and the combined correlation rule identified both failed and successful escalations, showing how an attacker might move from brute force to privilege gain.

Each detection was validated with screenshots, and the results were mapped against MITRE ATT&CK techniques (e.g. T1110 for brute force).

The lab showed how Wazuh can be customized to detect a range of attacks by tuning rules to match specific behaviors. It also highlighted that detection is not only about having a SIEM in place, but about understanding attacker behaviors and writing rules that connect events together. By simulating attacks in a controlled environment, I was able to see how alerts are generated, what the log sources look like, and where correlation rules provide the most value.

This project gave me hands-on experience with building detections in a SOC-like environment. I learned how to simulate attacks, write correlation rules, and validate results in Wazuh. The process reinforced the importance of detection engineering and made me more comfortable working with logs and SIEM tools. Going forward, I plan to expand this lab with more attack techniques and additional MITRE ATT&CK coverage.