Project 1: Security Monitoring & Incident Simulation Lab

Incident Report

Summary

A simulated security incident was conducted in a controlled lab environment to test monitoring, detection, and incident response capabilities using **Wazuh SIEM**. The scenario involved an attacker (Kali Linux) conducting an SSH brute-force attack and network reconnaissance against a victim server (Ubuntu LTS). The incident was successfully detected and logged in Wazuh, demonstrating effective SOC processes for identifying and responding to malicious activity.

Environment Setup

- **Attacker VM:** Kali Linux
- **Victim VM:** Ubuntu LTS with Wazuh Agent installed
- **SIEM VM:** Ubuntu Server running Wazuh Manager & Dashboard

Tools Used:

- **Attacker:** Hydra (SSH brute force), Nmap (network scanning)
- **Defender:** Wazuh SIEM (log collection, alerting, investigation)

Incident Timeline

Time (UTC)	Event	Source	Notes
10:05	Attacker initiated Nmap scan against victim	Kali Linux	Detected port scanning on port 22
10:07	Hydra brute-force attack launched	Kali Linux	Multiple failed SSH login attempts observed
10:08	Wazuh generated alert: *"Possible SSH brute-force attack"*	Wazuh Agent → SIEM	Alert severity: High

10:09	Wazuh correlation rule flagged multiple login failures	SIEM	Confirmed brute-force pattern
10:10	SOC investigation began	Analyst (me)	Reviewed logs, validated attack source
10:12	Attack confirmed as unauthorized access attempt	SOC	Escalated as Security Incident

---

Detection & Investigation

Wazuh Alert Logs:

- rule.id: 5710
- rule.level: 10
- description: Multiple SSH authentication failures (possible brute-force attack)
- srcip: 192.168.1.100 (attacker)
- dstip: 192.168.1.101 (victim)
- user: root

Additional Alerts:

- Port scanning activity (Nmap)
- Repeated failed logins from single IP

Validation:
Checked Wazuh dashboard → confirmed correlation rules triggered for brute-force pattern and port scanning.

Impact Assessment

- **Targeted Service:** SSH (port 22) on victim machine
- **Compromise Level:** None – attack was detected and blocked before successful login
- **Risk:** High (if password was weak, system could have been compromised)
- **Business Impact (simulated):** No real data loss, but in a production environment this could lead to unauthorized server access.

Response Actions

1. Detected malicious activity via SIEM alerts.
2. Investigated event details (source IP, attack pattern).
3. Escalated to incident status.
4. (Simulated) Blocked attacker IP using firewall rules on victim machine.
5. sudo ufw deny from 192.168.1.100 to any port 22
6. Recommended strengthening SSH access controls.

Lessons Learned

- **SIEM Value:** Wazuh successfully detected brute-force and port scan activities in real time.
- **Preventive Measures Needed:**
    - Enforce strong password policies.
    - Implement fail2ban or equivalent intrusion prevention.
    - Restrict SSH access to trusted IPs only.
    - Continuous monitoring with SIEM is critical for early detection.

Conclusion

This incident simulation demonstrated how an attacker's brute-force attempt and network reconnaissance can be detected by a SIEM. Wazuh provided timely alerts that allowed investigation and response, proving its effectiveness in a SOC workflow. The exercise highlights the importance of proactive monitoring, strong authentication, and rapid incident response.