Capstone Project: Full SOC Workflow Simulation

1. Objective

The objective of this capstone project is to simulate a full Security Operations Center (SOC) workflow. This includes attack simulation, detection, triage, response, containment, escalation, and reporting using industry-standard security tools and methodologies.

2. Lab Environment

- **Attacker Machine:** Kali Linux
- **Victim Machine:** Metasploitable2
- **Monitoring & Response Tools:**
    - Metasploit (Attack simulation)
    - Wazuh (Detection & alerting)
    - CrowdSec (Response & IP blocking)
    - TheHive (Incident escalation & case management)
    - Google Docs (Reporting & documentation)

3. Attack Simulation

Attack Performed

- Vulnerability exploited: **Samba usermap script vulnerability**

Metasploit module used:

```
exploit/multi/samba/usermap_script
```

- Target: Metasploitable2 Samba service

- Result: Remote code execution and shell access on the target system

Outcome

- Successful exploitation confirmed
- Unauthorized access achieved on the victim VM

4. Detection and Triage (Wazuh)

Wazuh detected abnormal Samba activity originating from an internal IP.

Alert Documentation

Timestamp	Source IP	Alert Description	MITRE Technique
2025-08-18 14:00:00	192.168.1.101	Samba exploit detected	T1210 – Exploitation of Remote Services

Triage Notes

- Alert severity: High
- Source IP correlated with Kali attacker
- Behavior matched known Samba exploitation patterns
- Alert confirmed as **True Positive**

5. Response and Containment

Actions Taken

1. **Victim VM Isolation**
    - Network interface disconnected to prevent lateral movement.
2. **IP Blocking via CrowdSec**
    - Attacker IP `192.168.1.101` added to CrowdSec blocklist.
3. **Verification**
    - Ping test from attacker to victim failed, confirming containment.

Result

- Attack traffic successfully blocked
- Further compromise prevented

6. Escalation

Case Summary

A high-severity security incident was identified involving the exploitation of a Samba service on a Metasploitable2 system. Wazuh detected abnormal activity corresponding to the Samba usermap script vulnerability (MITRE T1210). The attacker successfully gained unauthorized access from IP address 192.168.1.101. Immediate containment actions were taken, including isolating the affected virtual machine and blocking the malicious IP using CrowdSec. No evidence of lateral movement or data exfiltration was observed. The incident has been escalated to Tier 2 for deeper forensic analysis, validation of system integrity, and review of additional security hardening measures.

7. Incident Report

Executive Summary

On 18 August 2025, a simulated cyberattack was conducted against a Metasploitable2 system to evaluate SOC detection and response capabilities. The attack leveraged a known Samba vulnerability, resulting in unauthorized remote access. The SOC team successfully detected, contained, and documented the incident.

Timeline

- **14:00** – Samba exploit executed from attacker machine
- **14:01** – Wazuh generated high-severity alert
- **14:05** – Incident triaged and confirmed
- **14:10** – Victim system isolated
- **14:12** – Attacker IP blocked via CrowdSec

Recommendations

- Disable or remove vulnerable Samba services
- Apply system hardening and patch management
- Enhance IDS rules for lateral movement detection
- Conduct regular vulnerability assessments
- Provide administrator training on legacy service risks

8. Management Briefing (100 Words)

A simulated cyberattack was detected on one of our internal systems, where an attacker exploited a known network service vulnerability. The security monitoring system quickly identified the threat, and the affected system was immediately isolated to prevent further damage. The attacker’s access was blocked, and no sensitive data was compromised. This exercise confirmed that our monitoring and response processes are effective. To reduce future risk, we recommend removing outdated services, applying regular security updates, and continuing periodic security testing to strengthen our overall defense posture.