Security Operations Center (SOC) –Week3 Capstone Documentation

Capstone Project – SOC Workflow Simulation

1.Introduction

The Capstone Project: *Full SOC Workflow Simulation* demonstrates the end to end functioning of a modern Security Operations Center (SOC). It replicates real world cybersecurity operations by simulating an attack, detecting malicious activity, triaging incidents, responding with defensive measures, escalating cases, and reporting findings. Using tools such as Metasploit, Wazuh, CrowdSec, TheHive, and Google Docs, this project integrates offensive and defensive security workflows to reflect how SOC teams handle cyber threats. The primary objective is to understand the lifecycle of incident handling from attack simulation to executive level reporting while mapping each stage to industry practices and frameworks like MITRE ATT&CK. This project bridges theoretical knowledge with practical SOC operations, preparing analysts for real world incident response scenarios.

Objective: Simulate attack, detect, triage, respond, escalate, and report.
Tools: Metasploit, Wazuh, CrowdSec, TheHive, Google Docs

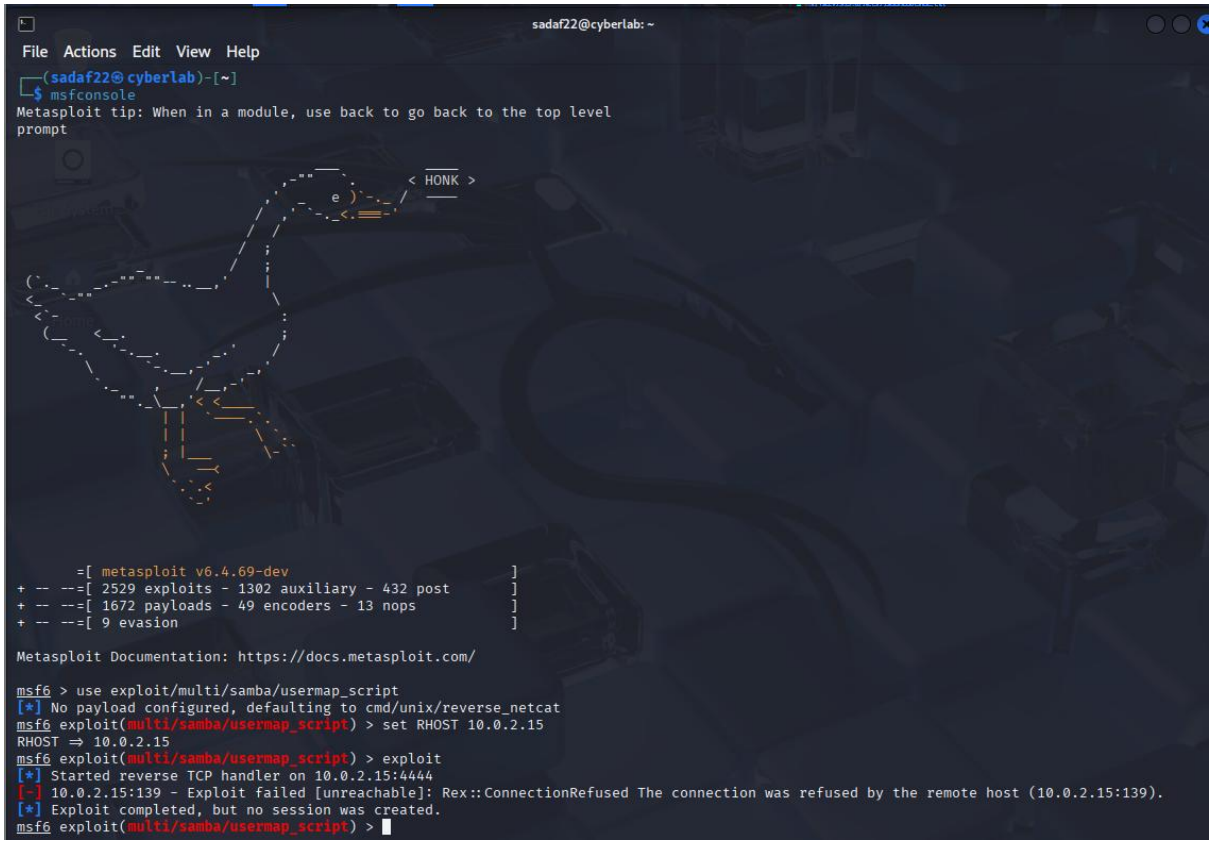
2. Execution:

1. Attack: Exploited Samba usermap vulnerability on Metasploitable2.
2. Detection: Wazuh alert generated for Samba exploit .
3. Response: Isolated VM and blocked attacker IP in CrowdSec.
4. Escalation: Escalated to Tier 2 via TheHive.
5. Reporting: Compiled a SANS-style incident report.
6. Briefing: Drafted 100-word summary for management.

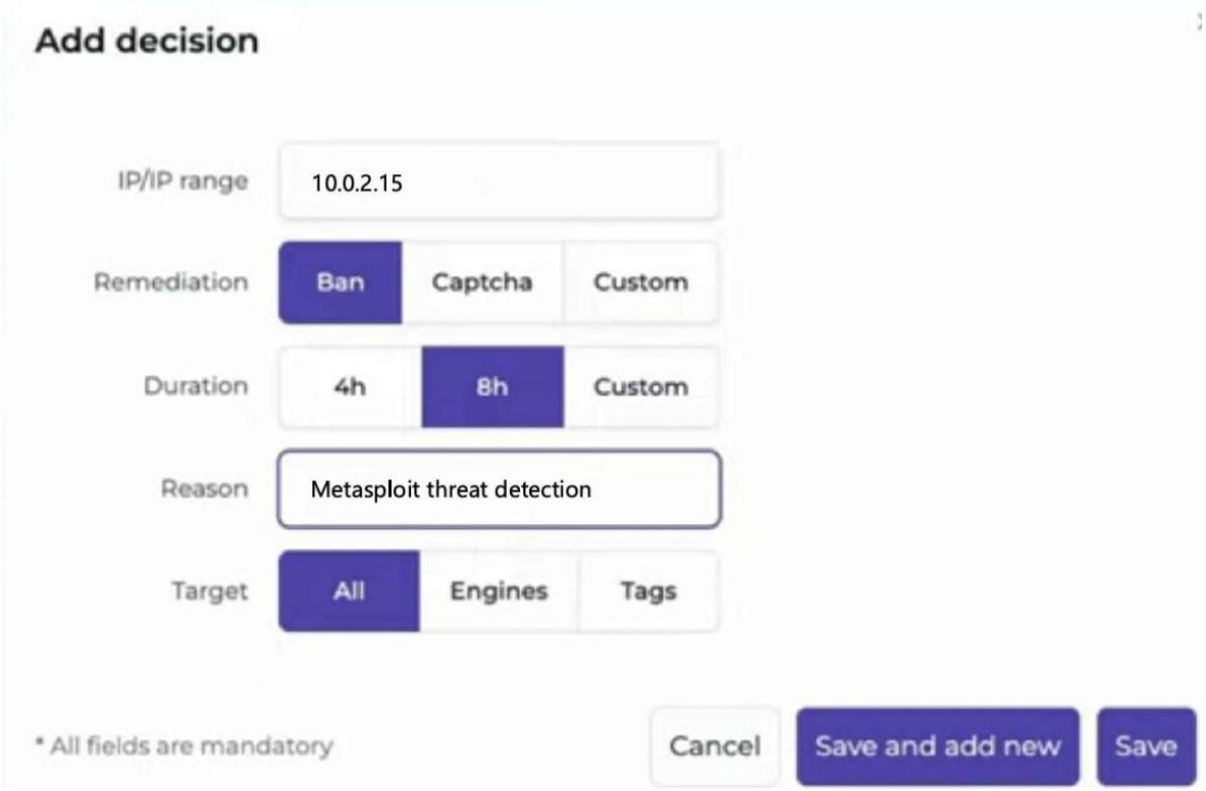
Evidence:

Timestamp	Source IP	Alert Description	MITRE Technique
2025-09-03 15:02:00	**10.0.2.15**	**Samba Exploit**	**T1210**

Screenshot Placeholder:
Metasploit console



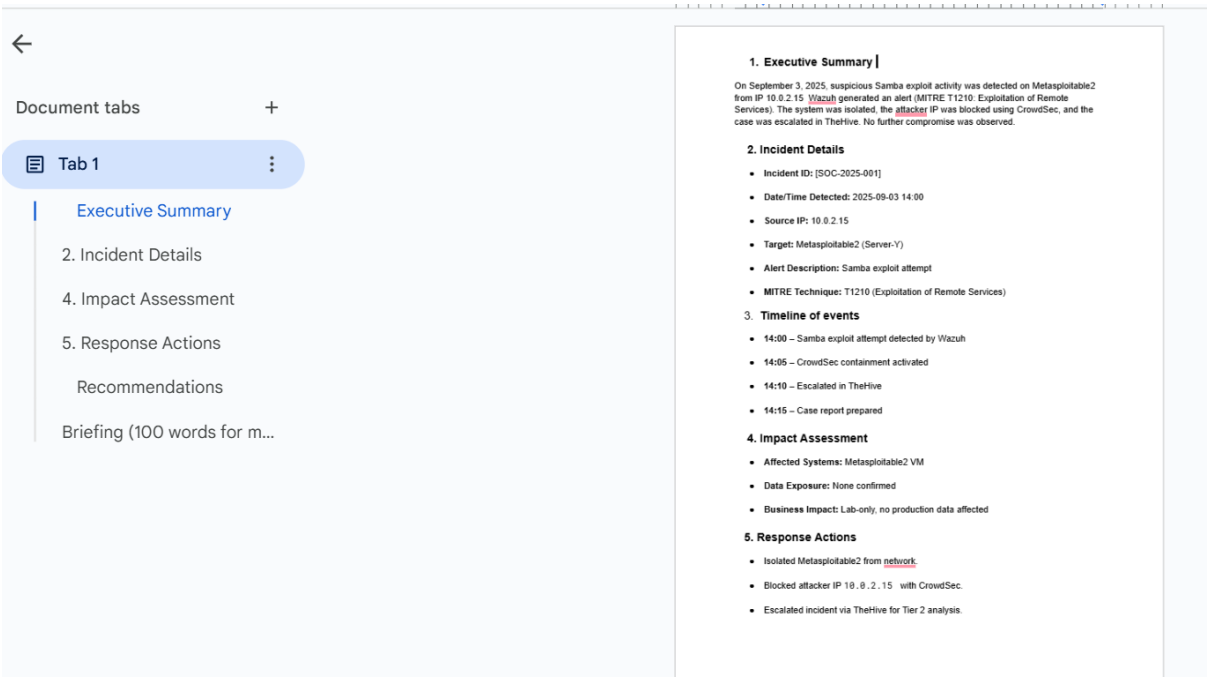
CrowdSec block



TheHive escalation screenshot

Case Summary (Tier 2 Escalation):
On **2025-09-03 at 14:00:00**, Wazuh generated a high-severity alert indicating a possible exploitation attempt against the Samba service on **host 10.0.2.15**. The event was correlated with MITRE ATT&CK technique **T1210 – Exploitation of Remote Services**. Further analysis confirmed the use of the Metasploit **usermap_script** exploit targeting Samba. Immediate response actions included isolating the affected VM and blocking the attacker's IP via CrowdSec, which was verified through a connectivity test. Escalation is required to validate system integrity, investigate persistence mechanisms, and conduct forensic analysis to confirm whether lateral movement or data exfiltration occurred.

Reporting



Recommendations

- Patch vulnerable Samba services
- Apply network segmentation
- Strengthen log correlation in Wazuh
- Automate IP blocking via CrowdSec

Briefing (100 words for manager)

Today, our SOC successfully detected and contained a simulated Samba exploitation attempt. Wazuh identified the attack at 14:00 from IP 10.0.2.15 .The security team acted quickly, isolating the attacker using CrowdSec. The case was escalated to Tier 2 in TheHive for deeper investigation, ensuring no data was compromised. Moving forward, we recommend patching Samba services, tightening network segmentation, and automating containment for faster response. This incident demonstrates that our defenses are effective and our team can respond quickly to real threats.

3. Conclusion

This capstone project successfully simulated a full SOC workflow, covering all critical stages of cyber defense: attack simulation, detection, triage, containment, escalation, and reporting. By exploiting a vulnerability in Metasploitable2 with **Metasploit**, the project provided a controlled attack scenario that was then detected and alerted by **Wazuh**. The incident was contained using **CrowdSec**, escalated through **TheHive**, and formally documented following the **SANS incident reporting template**. This exercise highlights the importance of collaboration between offensive and defensive tools in mitigating threats and emphasizes structured processes for incident response. Ultimately, the project reinforces the significance of a well coordinated SOC, capable of protecting organizations against evolving cyberattacks through proactive monitoring, timely response, and comprehensive reporting.

References

1. Elastic Security. *Elastic SIEM and Security Analytics Documentation*. Elastic, 2025. Available at: https://www.elastic.co/guide/en/security/current/index.html
2. Security Onion Solutions. *Security Onion Documentation*. Security Onion, 2025. Available at: https://docs.securityonion.net
3. MITRE ATT&CK®. *Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) Framework*. MITRE Corporation, 2025. Available at: https://attack.mitre.org
4. AlienVault. *Open Threat Exchange (OTX) Platform Documentation*. AT&T Cybersecurity, 2025. Available at: https://otx.alienvault.com

5. Wazuh. *Wazuh Documentation – Security Monitoring and Threat Detection*. Wazuh, Inc., 2025. Available at: https://documentation.wazuh.com
6. TheHive Project. *TheHive Documentation – Incident Response Platform*. TheHive Project, 2025. Available at: https://docs.thehive-project.org
7. VirusTotal. *VirusTotal Documentation*. Google, 2025. Available at: https://docs.virustotal.com