Capstone Project

1. Objective

This report contains the details of the task including Attack Simulation, Detection and Triage, Response and Containment, Escalation, Reporting, and Briefing. The goal of this task is to:

- Learn Full SOC Workflow Simulation it includes the attacking, detecting, response, reporting, And briefing.

2. Introduction

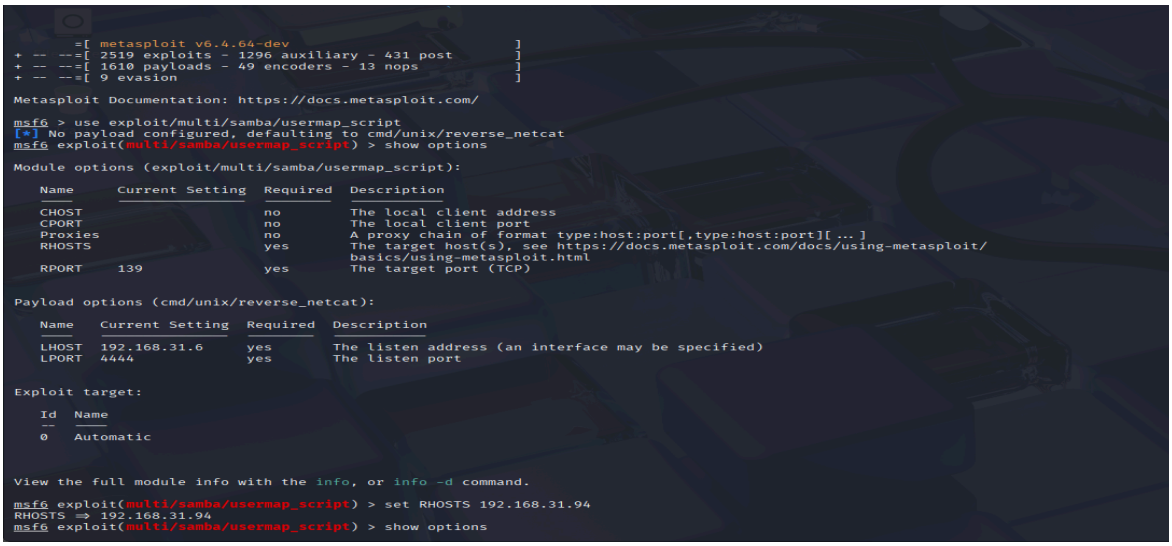
Capstone project it is a full SOC workflow simulation from the attack simulation to the last Briefing. It helps to learn how to perform attacks, how to detect them, when to respond, how to escalate it to higher authorities if needed, and how to write the report clearly.

3. Tools

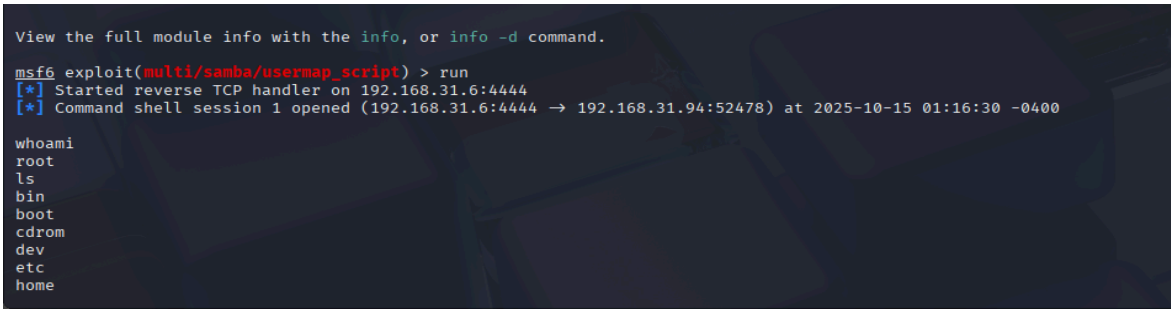
- Metasploit setup it using browser in Virtual Machine (VM Ware, Oracle Virtual Box). https://sourceforge.net/projects/metasploitable/
- Wazuh setup using its official documentation. https://documentation.wazuh.com/current/quickstart.html
- CrowdSec setup using its documentation. https://docs.crowdsec.net/
- TheHive setup using its documentation https://docs.strangebee.com/thehive/installation/installation-methods/
- Google Docs.

4. Attack Simulation

Performing an attack using Metasploitable2 and msfconsole in the Virtual Machine. Exploiting A Metasploitable2 vulnerability with Metasploit(e.g., Samba usermap script: use exploit/multi /samba/usermap_script). I performed the attack using msfconsole in the Kali Linux on the target Machine (Metasploitable2). I got the connection successfully. I exploited a vulnerability in the Metasplotable2.



A successful connection established from attack machine to target machine using the usermap Script.



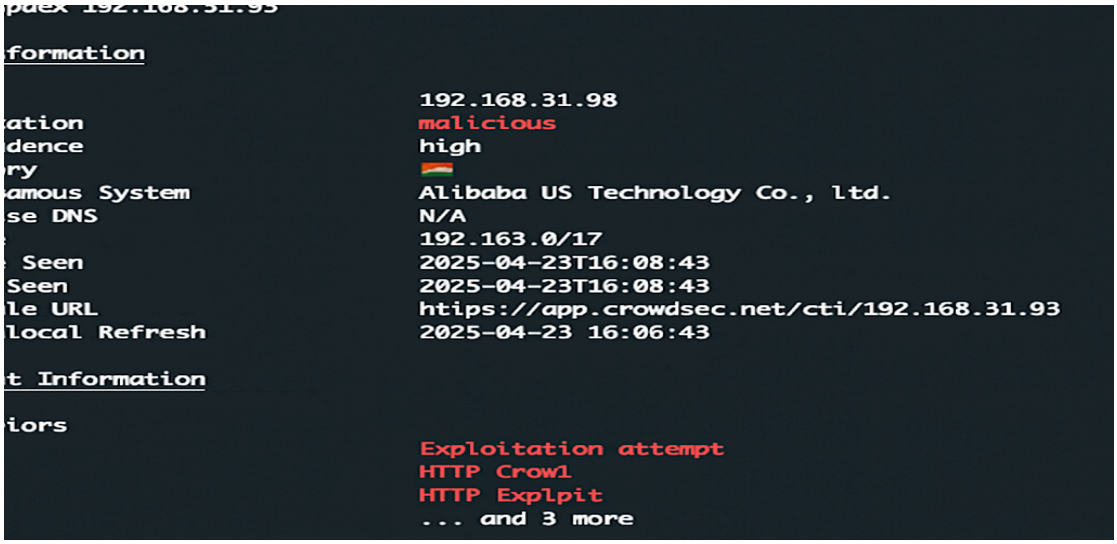
5. Detection and Triage

Detection and Triage means identifying the attack and finding whether the incident requires immediate response or not

@timestamp	Oct 23, 2025 @ 17:47:57.768
_index	wazuh-alerts-4.x-2025.10.23
agent.id	001
agent.ip	192.168.31.58
agent.name	Windows
decoder.name	syscheck_new_entry
full_log	File 'c:\users\karth\documents\logs sender\samba-logs.txt' added Mode: realtime
id	1761221877.314216
input.type	log
location	syscheck
manager.name	wazuh-server
rule.description	File added to the system.
rule.firedtimes	1
rule.gdpr	II_5.1.f
rule.gpg13	4.11

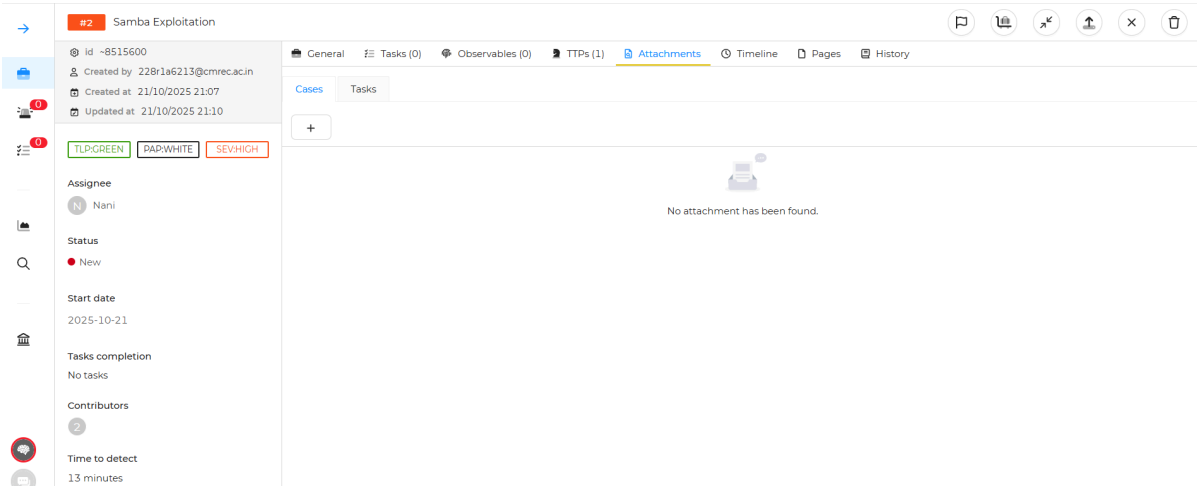
6. Response and Containment

Response means reacting to the incident to stop it from future effect. Containment is a process of isolating the affected system from the network to stop the spreading of attack on other systems. In this workflow after detecting and triaging the incident I responded and isolated VM And blocking the attacker's IP with the CrowdSec tool. And after isolation I tested the IP address by performing a ping test on it.



7. Escalation

Escalation is a process of sending the brief report to the higher authority if it is not suspended by the entry level analyst. For the further forensic investigation it is escalated to Tier 2 team. After responding and contaminating I escalated the incident via TheHive incident response tool to the Tier 2 team.



8. Reporting

Executive Summary:

On 16 October 2025 at 14:00:00 a Samba exploit against a Metasploitable2 VM was detected by Wazuh. The alert identified a Samba usermap script exploit (MITRE T1210) from 192.168.31.6. The VM was isolated, the attacker IP blocked via CrowdSec, and ping tests validated containment. The case was escalated to Tier 2 in TheHive for forensic analysis and remediation.

Timeline:

2025-10-16 14:00:00 — Wazuh alert: Samba exploit (T1210) from 192.168.3.6.
2025-10-16 14:05:00 — Containment: Metasploitable2 VM removed from network.
2025-10-16 14:10:00 — CrowdSec block applied to 192.168.3.6.
2025-10-16 14:12:00 — Ping confirms no connectivity.
2025-10-16 14:20:00 — Escalated to Tier 2 in TheHive.

Recommendations:

Fix or remove the vulnerable Samba service and make sure test VMs are kept separate.
Separate networks properly and limit exposure of SMB services to reduce risk.
Check and improve Wazuh alerts so attacks are detected faster and more accurately.
Save all forensic data (memory and disk) and investigate the cause of the attack thoroughly.

Prepared by: SOC Analyst

9. Briefing

Briefing is crucial because it is required to know the stakeholders how the incident happened and how it is mitigating and what actions need to be taken.

On 16 October 2025 at 14:00 an intrusion attempt targeted a Samba service on a lab VM. Wazuh detected the exploit originating from 192.168.3.6. The SOC isolated the VM, blocked the attacker IP with CrowdSec, and verified isolation with network tests. No production systems were affected and no lateral movement was observed. The case has been escalated to Tier 2 for forensic analysis and remediation planning. Recommended executive actions: approve patching

or removal of vulnerable services, confirm segmentation of test and production environments, and authorize forensic preservation and a brief credential reset for any exposed administrative accounts. Immediately.