Report: Capstone Project

Executive Summary

On 18 September 2025 at 14:00 UTC, the SOC conducted a controlled attack simulation against a Metasploitable2 host using Metasploit's Samba usermap_script exploit. The objective was to validate SOC workflows across detection, triage, containment, escalation, and reporting. The attack successfully established a reverse Meterpreter session, demonstrating compromise of the target system. Wazuh generated a high-priority alert mapped to MITRE Technique T1210 (Exploitation of Remote Services), which triggered incident handling processes. Containment was achieved by isolating the compromised VM and blocking the attacker IP via CrowdSec and firewall rules. Escalation was carried out by opening a TheHive case with supporting evidence.

Timeline

- 14:00 UTC: Exploit launched from 192.168.1.101 against 192.168.1.100.
- 14:01 UTC: Reverse shell established; proof file /tmp/pwned.txt created.
- 14:02 UTC: Wazuh alert triggered, mapped to MITRE T1210.
- 14:05 UTC: Incident triaged, VM isolated, attacker IP blocked via CrowdSec.
- 14:10 UTC: Escalation to Tier 2 in TheHive with logs, pcap, and hashes.

Recommendations

Apply patches or decommission vulnerable Samba services, enforce strict segmentation between lab and production, automate alert escalation from Wazuh to TheHive, and expand endpoint telemetry. Establish formal Tier-2 forensic workflows to ensure rapid imaging and analysis during real incidents.