Capstone Project – Full SOC Workflow Simulation

Attack Simulation

A simulated attack was conducted against a vulnerable Metasploitable2 virtual machine using the Samba usermap script vulnerability. The exploit was executed using Metasploit module exploit/multi/samba/usermap_script.

This vulnerability allows remote command execution due to improper handling of user input by the Samba service. The attack represents a real-world scenario where publicly exposed services are exploited by adversaries.

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

Detection and Triage Analysis

The attack was detected by the SIEM through abnormal process execution and service behavior associated with the Samba service. The alert was mapped to MITRE ATT&CK technique T1210 (Exploitation of Remote Services). Due to confirmed exploit behavior, the alert was triaged as High severity and escalated for response.

Response and Containment

Immediate containment actions were taken to prevent further compromise. The affected virtual machine was isolated from the network to stop lateral movement. The attacker's source IP address (192.168.1.101) was blocked using CrowdSec-based enforcement.

Containment effectiveness was verified by performing a ping test from the attacker machine, which confirmed loss of connectivity to the isolated system.

Escalation Summary

This incident was escalated to Tier 2 SOC following confirmation of a successful exploitation attempt on a Metasploitable2 system. The activity was detected at 14:00 IST and originated from IP address 192.168.1.101. Analysis identified exploitation of the Samba usermap script vulnerability, mapped to MITRE ATT&CK technique T1210. The affected system was isolated, and the source IP was blocked as part of containment. Further forensic analysis and validation of system integrity are required to assess potential persistence or data exposure.

Executive Summary

On 18 August 2025, a simulated exploitation attempt was detected against a vulnerable Samba service hosted on a Metasploitable2 virtual machine. The incident was identified through SIEM alerting and mapped to a known remote service exploitation technique.

Timeline

At 14:00 IST, an alert was generated indicating abnormal Samba service behavior. Initial triage confirmed an exploit attempt originating from IP address 192.168.1.101. The incident was escalated for immediate response.

Response and Recovery

The affected system was isolated to prevent lateral movement. The attacker’s IP was blocked using CrowdSec controls. System logs and artifacts were preserved for further analysis. No evidence of persistent compromise was identified.

Recommendations

It is recommended to restrict unnecessary public services, apply timely security patches, implement intrusion prevention controls, and continuously monitor exposed services to reduce exploitation risks.

Stakeholder Briefing

A simulated security incident involving an attempted system compromise was detected and contained promptly. The affected test server was isolated, and the suspicious external IP address was blocked. No business systems or data were impacted. The incident was resolved quickly due to effective monitoring and response procedures. Preventive measures are being reinforced to reduce the risk of similar incidents in the future.