Title: SANS-Style Incident Report (300 Words)

Date: 24 Nov 2025
Prepared by: Mayuri Sawle

Executive Summary
A targeted exploitation attempt was executed on the Metasploitable2 environment using a Samba usermap vulnerability. Monitoring tools detected the attack, triggering automated triage and containment. The SOC successfully isolated the affected system and prevented lateral movement.

Incident Timeline

- 16:00 – Metasploit exploitation launched
- 16:05 – Wazuh generated high-severity alert
- 17:45 – TheHive triage completed
- 18:00 – CrowdSec automatically blocked attacker IP
- 22:00 – Full remediation completed

Root Cause Analysis
The attack succeeded because the Samba service on the target VM was unpatched. RCA revealed that the asset was missing from the official inventory and was therefore not included in patching cycles. A lack of automated asset-discovery processes contributed to the visibility gap.

Technical Analysis
Caldera was used to emulate remote-service exploitation (T1210). Wazuh successfully detected the activity but relied heavily on static signatures. Behavioral analytics coverage for lateral movement was found to be limited. Response was enhanced with automated IP blocking via TheHive–CrowdSec integration.

Metrics:
MTTD = 2 hours
MTTR = 4 hours
Dwell Time ≈ 6 hours

Recommendations

1. Implement continuous asset discovery.
2. Patch vulnerable Samba services and legacy assets.
3. Strengthen behavioral detection rules in Wazuh.
4. Expand SOAR automation for containment and ticketing.
5. Conduct quarterly red-team/blue-team exercises.