
Capstone Report

Executive Summary

On February 12, 2026, a controlled Security Operations Center (SOC) capstone exercise was conducted to validate end-to-end incident response capabilities. A simulated exploitation of a vulnerable Samba service was performed against a lab environment using Metasploit. Detection was achieved within seconds through Wazuh integrated with Elastic Security. Automated case creation and containment actions significantly reduced attacker dwell time. The incident lifecycle, from initial compromise to containment, was completed within 69.75 minutes. Root cause analysis identified outdated software and lack of network segmentation as key contributing factors. Remediation actions were defined to strengthen resilience and reduce future exposure.

Timeline

13:30:54 – Exploit initiated against vulnerable Samba service
13:31:02 – Wazuh high-severity alert generated
13:32:15 – Case automatically created in TheHive
13:40:10 – Malicious source IP blocked via CrowdSec
14:40:39 – Containment verified; incident response completed

Root Cause Analysis

Primary Cause: Exposure of vulnerable Samba 3.0.20 service.

Contributing Factors:

- No patch management process for lab systems
- Absence of network segmentation
- Lack of preventive hardening controls

Recommendations

1. Implement structured patch management across all environments.
2. Enforce network segmentation between training and operational assets.
3. Conduct routine vulnerability assessments.
4. Expand automated containment playbooks for high-severity alerts.