Title: Incident Response Template (SANS-Based SMB Brute Force on Windows 10 VM)

Prepared by: Mayuri Sawle
Date: 25 Nov 2025

1. Executive Summary

A simulated SMB brute-force attack was performed on a Windows 10 test machine. Multiple failed authentication attempts were detected by Wazuh, and the SOC team initiated containment and evidence collection. No successful login occurred, and the system was isolated to prevent further attempts.

2. Timelines of Events

Time	Event
14:00	Metasploit detected SMB brute-force attempts
14:05	SOC isolated Windows 10 endpoint
14:30	Memory acquired for investigation

3. Impact Analysis (Brief)

The Windows 10 system experienced repeated login failures over SMB. No credential compromise was observed. No lateral movement, data access, or system modification occurred.

4. Remediation Steps

- Block attacker IP in firewall/CrowdSec
- Disable SMBv1 if enabled
- Enforce strong password policy
- Review failed login thresholds
- Reset affected user passwords (if required)

5. Lessons Learned

Enhance brute-force alert tuning, enforce MFA, and monitor authentication logs more aggressively.