Title: Capstone Report (Smb brute force Exploit)

Prepared by: Mayuri Sawle
Date: 25 Nov 2025

Executive Summary:
A controlled security assessment was conducted to evaluate our detection and response readiness against brute-force authentication attacks. Using Metasploit, an SMB brute-force attempt was launched against a Metasploitable2 test server with the victim IP 10.178.124.51. Wazuh successfully identified repeated failed login attempts and generated alerts mapped to MITRE Technique T1110 (Brute Force). The incident validated the SOC's capability to detect credential-based attacks and execute timely response actions.

Timeline:
At 11:00 AM, the attacker IP 192.168.1.102 initiated an SMB brute-force sequence targeting the victim system 10.178.124.51. Wazuh flagged multiple authentication failures within seconds, triggering an automated medium-severity alert. The SOC team began triage, verified the activity as malicious, and confirmed it originated from the test lab environment. By 11:15 AM, the victim VM was isolated, and CrowdSec was used to block the attacker's IP. A follow-up ping test confirmed that the network-level block was successful.

Recommendations:
Strengthen detection thresholds for SMB authentication anomalies and enable automatic IP blocking for repeated failures. Enforce strong password policies and restrict SMB exposure to necessary hosts only. Maintain regular patching of SMB services, enhance alert correlation rules, and continue SOC analyst training to improve response time for brute-force attack attempts.