Final Capstone Report – SMB Brute-Force Incident

Project Title: Capstone Incident Response – SMB Brute-Force Attack
Prepared by: Abhishek Tiwary – SOC Analyst (Tier 1)
Date: 11 Oct 2025

A. Executive Summary

An SMB Brute-Force attack (**MITRE ATT&CK T1110**) targeting the Windows 10 VM (Victim IP: **10.178.124.51**) was successfully detected and contained on **11 Oct 2025**. The attack originated from the Attacker VM and was instantly flagged by the **CrowdSec agent**. The automated response system issued a **BAN decision**, preventing further unauthorized access. Containment was verified via a **failed ping test**, confirming complete isolation of the attacker.

B. Timeline & Procedures

The incident was identified at **T+0:00** when repeated failed SMB logins (**Event ID 4625**) were detected. By **T+0:30**, the **CrowdSec Server** issued a BAN decision against the attacker IP (**10.178.124.51**). At **T+0:45**, containment was confirmed through a failed ping test, proving the firewall's effectiveness. However, **Velociraptor forensic acquisition** for volatile data and memory dump failed due to **VM kernel incompatibility**, limiting evidence collection.

C. Recommendations

Policy Hardening: Enforce strong Windows Account Lockout Policy and disable unused SMB services where possible.
Mitigate Constraint: Use supported and stable Windows 10/11 Evaluation Images for reliable operation of IR tools like **Velociraptor**.
Auditing: Conduct a detailed review of Windows Event Logs and firewall decisions to verify no residual unauthorized activity remains post-containment.