Investigation Steps Log (Incident Timeline)

File Name: 2.2_Investigation_Steps_Log.pdf
Incident: SMB Brute-Force Attack on Windows 10 VM
Analyst: Abhishek Tiwary – SOC Analyst (Tier 1)

Incident Response Lifecycle: Identification & Containment Phase

Timestamp (Mock)	Action ID (Incident Phase)	Action Description (What happened?)	Verification / Proof
T + 00:00:00	Detection / Alert	SMB Brute-Force Attack initiated from Attacker VM (10.178.124.51) targeting Windows 10 VM.	Metasploit auxiliary module (**smb_login**) execution began.
T + 00:00:15	Identification / Data Ingest	Windows 10 Agent (CrowdSec) detected multiple failed authentication attempts (**Event ID 4625**).	Logs successfully transmitted to Kali LAPI (Local API).
T + 00:00:30	Decision / Containment	CrowdSec Server issued **BAN decision** against Source IP (10.178.124.51).	`cscli decisions list` showed **Active Ban (Duration: 4h)**. *(Proof Screenshot required)*
T + 00:00:45	Response / Verification	SOC Analyst executed a **Ping Test** from Attacker VM to Victim VM (10.178.124.51).	Connection **FAILED** — Network-level containment successfully applied by Firewall Bouncer. *(Proof Screenshot required)*

T + 00:01:00	Evidence / Triage	Attempted **Volatile Data Collection** (Netstat/Memory Dump) using Velociraptor.	Acquisition **Failed** (Documented due to VM kernel incompatibility).
T + 00:10:00	Eradication / Documentation	Incident documented in Google Docs/Ticket Draft; Attacker IP added to external watchlist.	Documentation completed and **Tier 2 Escalation Email** drafted.

Prepared by: Abhishek Tiwary – SOC Analyst (Tier 1)
Date: 11 Oct 2025