Final Capstone Reports

A. **Document Name**

Task 6: Final Incident Reports and Briefing

B. **Purpose**

This document provides both a non-technical manager briefing and a formal incident report summarizing the Capstone project outcomes, from detection to containment and recommendations.

1. Manager Briefing (Non-Technical – 100 Words)

A security alert was raised when a Windows 10 computer attempted to communicate over an encrypted channel that appeared suspicious. Further investigation showed that an unauthorized remote connection—often called a "reverse shell"—had been briefly established. Our team immediately blocked the attacker, isolated the computer, and confirmed that no sensitive systems or data were affected. The situation is fully contained. A specialized team is now performing a deeper review to ensure nothing else occurred. We are strengthening monitoring and adjusting security controls to prevent similar incidents in the future.

2. Final Incident Report (Technical – 200 Words)

Title: CRITICAL INCIDENT: Meterpreter Reverse Shell (MITRE T1573)

Detection Findings:
At 14:00:05 on August 18, 2025, Wazuh detected suspicious encrypted outbound communication from the Windows 10 workstation consistent with MITRE T1573 (Encrypted Channel). Shortly thereafter, a reverse shell payload was executed on the host, mapped to T1059 (Execution). These correlated alerts indicated active unauthorized remote control.
Updated Timeline (partial):

- 14:00:05 – Wazuh detects encrypted C2-like traffic from Win10 host.
- 14:00:05 – Reverse shell execution alert generated.
- 14:02 – Analyst confirms malicious behavior.
- 14:05 – CrowdSec blocks attacker IP; host isolated.