Document 8: 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)

Team, we successfully detected and contained a sophisticated malware attack that briefly compromised a testing workstation. The automated security system flagged the unauthorized execution of a malicious file, indicating a high-risk security event. We immediately isolated the affected machine from the network, successfully eliminating the attacker's access. There was zero evidence of lateral movement or data loss. The system is now contained, and we are proceeding with forensic analysis to determine the root cause and prepare the machine for remediation. The risk has been neutralized.

---

2. Final Incident Report (Technical – 200 Words)

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

Executive Summary:
On 2025-08-18, a Windows 10 workstation was compromised via user execution of a reverse TCP payload, resulting in a live Meterpreter session. Wazuh successfully detected the intrusion by monitoring process creation and outbound C2 communication attempts (T1573). The threat was contained within 30 seconds, with no signs of lateral movement or data exfiltration.

Timeline:

- 14:00:00 IST: Payload executed.
- 14:00:05 IST: Wazuh rule triggered on suspicious outbound C2 connection.
- 14:00:20 IST: Containment action initiated (UFW block), terminating the session.

Actions Taken:

- Attacker IP blocked (CrowdSec simulation).
- Velociraptor memory dump and volatile data preserved; SHA256 hash recorded for integrity.

- Incident escalated to Tier 2 for full root cause analysis and forensic review.

Recommendations:

1. Implement application whitelisting (AppLocker) to prevent unauthorized execution.
2. Conduct phishing and executable awareness training for end users.
3. Re-image the affected workstation and review access controls before redeployment.