Document 5: Escalation Summary (Task 3.1 & 6.4)

A. Document Name
Task 3 & 6: Incident Escalation Summary (Tier 2 Handover)

B. Purpose
This summary serves as a Tier 1 Analyst handover note to the Tier 2 team in TheHive, providing details of the simulated Capstone attack involving a reverse shell. It includes detection evidence, initial containment actions, and recommendations for deeper investigation.

C. Summary (100 Words)
Incident Summary: Critical Reverse Shell Foothold – Win10-Victim

A critical Meterpreter reverse shell session (MITRE T1573) was detected originating from Win10-Victim on port 4444, indicating successful initial access through execution of a malicious payload. Containment: The client IP was immediately quarantined and blocked using ufw, simulating a CrowdSec response, which terminated the active session. The incident has been escalated to Tier 2 for complete root cause analysis, identification of any persistence mechanisms, and system image remediation. A Velociraptor memory dump has been preserved and is available for detailed forensic investigation**.**