Capstone Detection and Triage Table (Task 6.2)

A. Document Name

Task 6: Capstone Detection and Triage Table

B. Purpose

During a controlled lab exercise, a vulnerability in **Metasploitable2** was targeted using a known Samba-related exploit module. The activity was run in a fully isolated virtual environment for training purposes only. The objective was to simulate an adversary gaining unauthorized remote access to trigger SOC monitoring, incident response, and escalation workflows. The attack generated network activity and suspicious authentication attempts observable in Wazuh.

C. Detection Table

Timestamp	Source IP	Alert Description	MITRE Technique(s)
2025-08-18 14:00:05	[Win10-Victim IP]	Suspicious C2 channel / Reverse Shell activity	T1573 (Encrypted Channel), T1059 (Execution)

D. Notes / Triage Actions (brief)

- Verify the source IP and host details in the inventory.
- Quarantine the host and block outbound port 4444.
- Preserve memory and network captures for forensic analysis.
- Escalate to Tier 2 for persistence hunting and full remediation.