Document 1: Log Correlation Table (Task 1.2)

A. Purpose

To show that the monitoring system (Wazuh) links a local user action (Failed login — Windows Event ID **4625**) with a network consequence (outbound network activity — Wazuh Event ID **61109**). This proves endpoint and network correlation for incident detection.

B. Log Correlation Table

Timestamp	Event ID	Source IP	Destination IP	Notes
2025-10-21 10:45:12	4625	10.239.143.25	N/A	Correlated: Failed interactive login on the Windows 10 VM.
2025-10-21 10:45:15	61109	10.239.143.25	8.8.8.8	Suspicious outbound DNS/network request observed immediately after the failed login. Possible beaconing or automated process.

C. Short explanation / significance

- **4625 (Failed Login):** Recorded when an interactive login attempt fails. Can indicate brute-force attempts, credential errors, or an attacker probing accounts.
- **61109 (Network Activity):** Wazuh rule showing outbound network activity to an external IP (here `8.8.8.8`).
- **Why it matters:** The two events occur within seconds of each other from the same source IP. That timing and IP match suggest the failed login and the outbound request are related — this linkage is important for detecting early-stage compromise (e.g., an automated process that triggers network callbacks after authentication attempts).