◆ L2 ANALYST REPORT

Deep Analysis

- Reviewed firewall logs and dashboards
- Confirmed repeated TCP connection attempts
- Behavior aligns with MITRE T1046
- No evidence of exploitation yet

Risk Assessment

- Severity: Medium
- Impact: Reconnaissance phase only
- Threat Type: Internal scanning

Recommendations

- Block or isolate source IP
- Review endpoint activity on attacker system
- Monitor for lateral movement
- Retain logs for future correlation

Incident Status

Confirmed Reconnaissance – Closed (Monitored)