🚨 INCIDENT ESCALATION REPORT (SOC L1 → L2)

🔹 Incident Title

Internal Port Scan Detected

🔹 L1 ANALYST REPORT

Date/Time: 2026-01-XX

Detection Source: Splunk SIEM

Alert Name: SOC – Internal Port Scan Detection

Summary

Splunk alert triggered indicating potential reconnaissance activity from an internal IP attempting connections to multiple destination ports on a Windows host.

Observations

- **Source IP:** 192.168.56.104
- **Destination** Host: 192.168.56.105
- **Event IDs:** 5156, 5157
- **Distinct ports accessed:** ≥ 3
- Tool suspected: Nmap , Nessuss

Initial Assessment

Activity appears consistent with port scanning behavior.

Action Taken

- Validated source IP
- Confirmed activity not part of normal operations
- Escalated to L2 for further investigation

Status: Escalated