SOC Use Case Report

UC-019: Detecting Network and Port Scanning

Author	Abishek V
Date	2 Feb 2026
Environment	Home SOC Lab (VirtualBox)
Primary Logs	Firewall / Network Telemetry
Target OS	Windows 10

1. Use Case Summary

Use Case ID	UC-019
Use Case Name	Detecting Network and Port Scanning
Category	Reconnaissance / Network Discovery
SOC Tier	L1 (Triage + Investigation)
Severity Guideline	Medium → High

Port scanning is commonly used during reconnaissance to identify open services and attack surface. SOC L1 must quickly determine whether scanning activity is benign or indicative of malicious intent.

2. Scenario

- Target endpoint: Windows 10 (`192.168.56.110`)
- Source host: Kali Linux (`192.168.56.120`)
- Activity observed: Multiple connection attempts to different ports
- Scan type: TCP SYN scan

SOC risk point: Unauthorized scanning often precedes exploitation or lateral movement.

3. Telemetry and Evidence

Primary logs

- Firewall logs
- Network flow telemetry
- IDS/IPS alerts (if available)

Key Indicators

Multiple Dest Ports	Rapid sequential connections
Single Source IP	Same source scanning many ports
Short Time Window	High connection rate

4. Detection Logic

Trigger when:

- a single source attempts connections to many ports
- connection attempts exceed normal baseline within short time window

Common thresholds:

- 20+ unique destination ports within 1 minute
- repeated connection failures from same source

5. SOC L1 Playbook

Phase A: Triage

1. Identify source and destination IPs
2. Identify time window and number of ports scanned
3. Check whether source is internal or external

Phase B: Investigation

1. Identify scan pattern (horizontal vs vertical)
2. Validate if scanning source is authorized
3. Check for follow-on exploitation attempts
4. Scope scanning activity across other hosts

6. Evidence Timeline

Time	Source IP	Destination	Observation
03:26:12	192.168.56.120	192.168.56.110:22	Connection attempt
03:26:13	192.168.56.120	192.168.56.110:80	Connection attempt
03:26:14	192.168.56.120	192.168.56.110:445	Connection attempt
03:26:20	192.168.56.120	Multiple ports	Sequential scan pattern

Outcome: Unauthorized port scanning activity detected from internal source. Classified as reconnaissance.

7. False Positive Checks

- vulnerability scanner or asset discovery tool
- monitoring or health-check services
- authorized penetration testing

8. Verdict Criteria

True Positive if:

- scanning source is unauthorized
- scan pattern matches reconnaissance behavior
- activity aligns with other suspicious indicators

Unauthorized scanning activity should be escalated if followed by exploitation attempts.

9. SOC Response Actions

- block or rate-limit source IP if required
- notify network/security teams
- monitor target hosts for exploitation attempts
- document source behavior for future correlation

10. Ticket Notes

Ticket: UC-019 Network and Port Scanning Detected
Severity: Medium
Verdict: True Positive (Reconnaissance)

Analyst Notes

- Observed high-rate connection attempts to multiple ports from single source IP.
- Scan pattern consistent with TCP port scanning.
- No exploitation observed at time of investigation.