SOC Use Case Report

UC-020: Identifying Port Scanning Activity

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

1. Use Case Summary

Use Case ID	UC-020
Use Case Name	Identifying Port Scanning Activity
Category	Reconnaissance / Network Discovery
SOC Tier	L1 (Triage + Investigation)
Severity Guideline	Medium

Port scanning activity focuses specifically on identifying open or exposed services on a single host or subnet. SOC L1 must determine intent, scope, and whether the activity is authorized.

2. Scenario

- Target endpoint: Windows 10 (`192.168.56.110`)
- Source host: Kali Linux (`192.168.56.120`)
- Activity observed: Sequential probing of common service ports
- Scan focus: Single host, multiple ports

SOC risk point: Focused port scanning often indicates targeting prior to exploitation.

3. Telemetry and Evidence

Primary logs

- Firewall allow/deny logs
- Network flow (NetFlow/Zeek equivalent)
- IDS alerts (if present)

Key Indicators

Repeated SYN Attempts	Connection attempts without full handshake
Sequential Ports	Ordered or patterned port access
Single Destination	One host repeatedly targeted

4. Detection Logic

Trigger when:

- a single source probes many ports on one destination
- connection attempts exceed normal service behavior

Typical baseline:

- 15+ unique ports within 60 seconds
- majority of attempts result in reset or timeout

5. SOC L1 Playbook

Phase A: Triage

1. Identify source IP and target host

2. Count number of unique destination ports
3. Identify scan duration and rate

Phase B: Investigation

1. Classify scan type (SYN, connect, service probe)
2. Validate whether source is authorized
3. Review target exposure (open services)
4. Check for exploit attempts following scan
5. Scope for similar scans across environment

6. Evidence Timeline

Time	Source IP	Destination Port	Observation
04:02:11	192.168.56.120	21	Connection attempt
04:02:12	192.168.56.120	22	Connection attempt
04:02:13	192.168.56.120	80	Connection attempt
04:02:18	192.168.56.120	Multiple	Sequential probing pattern

Outcome: Port scanning activity detected targeting a single endpoint. No exploitation observed.

7. False Positive Checks

- authorized vulnerability scanning
- asset discovery tools
- internal monitoring checks

8. Verdict Criteria

True Positive if:

- scanning source is unauthorized
- scan pattern matches reconnaissance behavior

Repeated port scanning should be monitored for escalation into exploitation.

9. SOC Response Actions

- log and track source IP behavior
- notify network team if repeated
- apply firewall blocks if risk increases
- monitor target services closely

10. Ticket Notes

Ticket: UC-020 Port Scanning Activity
Severity: Medium
Verdict: True Positive (Reconnaissance)

Analyst Notes

- Detected sequential probing of multiple ports on a single host.
- Activity consistent with port scanning reconnaissance.
- No exploit attempts identified at time of analysis.