

Rule Report — rule-4e8bb74c

Created: 2025-10-03T08:27:57Z | Threat Level: Medium

Executive summary: Detected FIN_SCAN from 10.129.5.193 targeting N/A.

Technical summary

Field	Value
Rule ID	rule-4e8bb74c
Alert Type	FIN_SCAN
Src IP	10.129.5.193
Target IP	N/A
Ports	1025, 110, 111, 113, 135, 139, 143, 1720, 1723, 199, 21, 22, 23, 25, 256
CVSS	3.6
Risk score	58.0 (Medium)
Decision	notify — FIN_SCAN detected (low priority - monitoring)

Correlation / Related alerts

Related alerts (last 48h): **56**



Enrichment

Country	N/A
City	N/A
Reputation Score	0.5
IP Info Raw	None

Evidence

Raw alert: `{"alert type": "FIN SCAN", "src ip": "10.129.5.193", "target ip": null, "ports": ["1025", "110", "111", "113", "135", "139", "143", "1720", "1723", "199", "21", "22", "23", "25", "256"], "start_time": "Mon Jun 2 13:29:17 2025", "duration": null}`

Capture Time: Mon Jun 2 13:29:17 2025

Created by: rule-generator | Reviewed by: N/A | SHA256: 185a0da114e19029649dd1c8964e3724397aa2d35b43b9ea651da289757ef233