

Network Traffic Security Analysis Report

Executive Summary

Network Traffic Analysis Security ReportExecutive Summary

1,000 instances of TCP connect scans detected from external IPs targeting internal host 192.168.100.99.

Critical traffic spike: Internal IP 192.168.100.99 transmitted 929 packets in a single minute (14:07 on 2025-03-20), exceeding the 60.55-packet threshold by 1,433%.

Bidirectional anomalous traffic observed between internal IP 192.168.100.99 and multiple external IPs, suggesting potential lateral movement or compromised system behavior.

Risk Assessment

Critical Risks (■)

Host compromise likelihood: Internal IP 192.168.100.99 shows both inbound attack targeting (SYN scans) and outbound anomalous traffic patterns.

Potential data exfiltration: 929 packets from internal IP in 60 seconds could represent ~**15.48 MB data transfer** (assuming 1,500B/packet).

Reconnaissance activity: 1,000 TCP SYN scans with window sizes >1024 indicate systematic network probing.

High Risks (■)

Unanswered TCP scan attempts from external IPs (63.2.154.223, 68.51.139.235, 136.237.33.61) could escalate to exploitation.

Lack of protocol-layer attacks (0 TCP/UDP/ICMP/ARP attack packets) suggests attackers are still in reconnaissance phase.

Threat Observations

TCP Connect Scans

Pattern: SYN flags with window sizes >1024 from 3 distinct external IPs

Target: 100% of scans directed at 192.168.100.99

Technical significance: Large window sizes may bypass legacy IDS systems using default scan detection thresholds

Temporal Anomaly

Internal host behavior: 192.168.100.99 transmitted 929 packets in 1 minute:

15.3x above normal baseline

Simultaneous inbound scans and outbound traffic suggests possible C2 communication

Protocol distribution: 100% TCP traffic during anomaly window

Traffic Correlation

Bidirectional communication observed between 192.168.100.99 and scanning IPs:

Packet 39 (inbound scan) → Packet 40 (outbound anomaly)

Packet 42 (inbound scan) → Packet 44 (outbound anomaly)

Recommendations

Immediate Actions

Quarantine 192.168.100.99: Initiate host isolation and conduct memory forensics

Block external IPs at firewall: 63.2.154.223, 68.51.139.235, 136.237.33.61

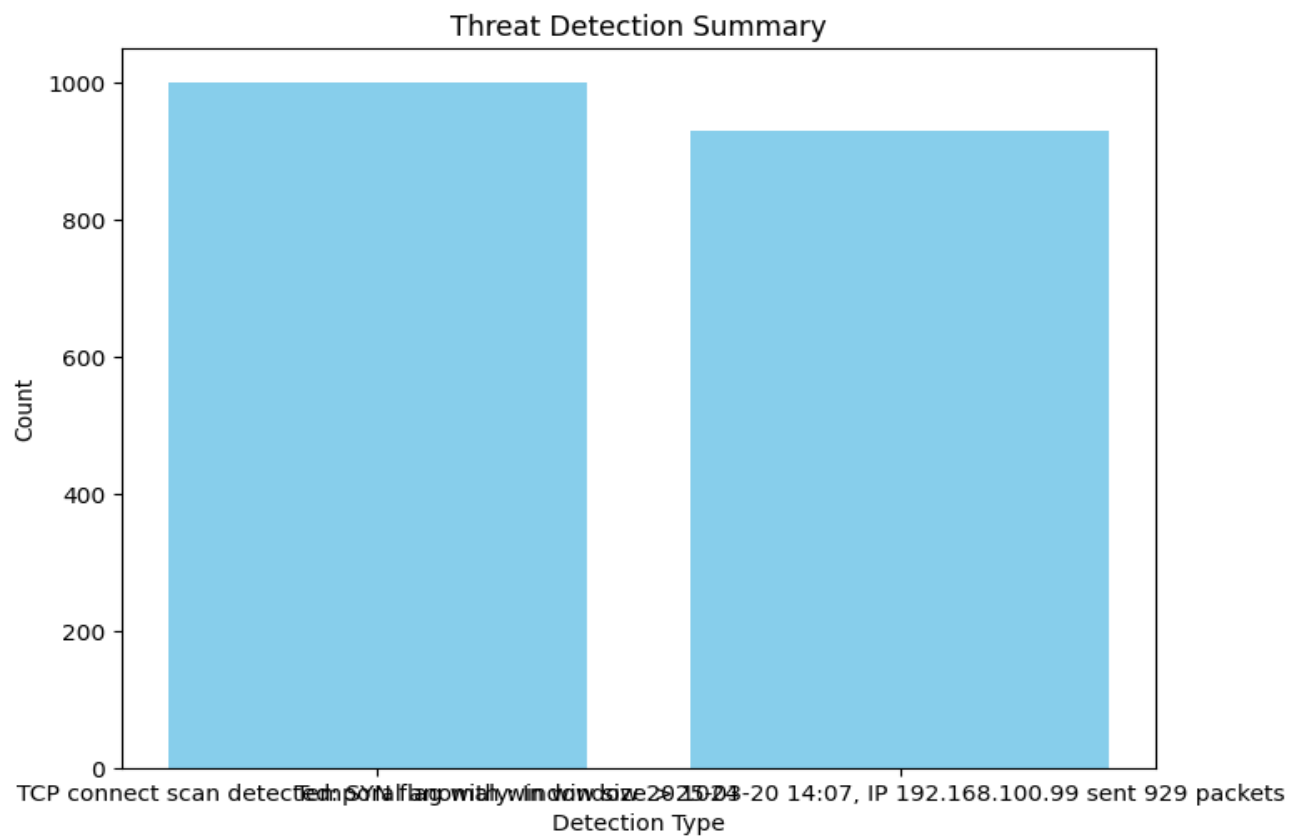
Deploy network segmentation: Limit east-west traffic for critical subnets
Technical Controls

Update IDS/IPS rules to detect:
tcp.window_size > 1024 and tcp.flags.syn == 1
Threshold alerts for hosts exceeding 50 packets/minute
Implement egress filtering for internal hosts
Enable TCP RST challenge for unsolicited SYN packets
Investigation Priorities

Review 192.168.100.99 for:
Scheduled tasks/cron jobs
Unknown listening ports
Recent privilege escalation events
Analyze full packet captures between 14:07-14:08 for payload patterns
Verify SIEM correlation rules for scan → traffic spike sequences
Long-Term Improvements

Conduct purple team exercise simulating scan/exfiltration patterns
Deploy network traffic baselining tools
Implement strict outbound connection whitelisting

Threat Detection Summary



Detection Type	Count
TCP connect scan detected: SYN flag with window size > 1024	1000
Temporal anomaly: In window 2025-03-20 14:07, IP 192.168.100.99 sent 929 packets (threshold=60.55)	929