Network Traffic Security Analysis Report

Executive Summary

Network Traffic Analysis Security ReportExecutive Summary

1,000 instances of TCP connect scans detected within a single monitoring window, indicating active reconnaissance activity targeting internal host 192.168.100.99.
No malicious TCP/UDP/ICMP/ARP packets observed beyond the TCP scan alerts.
Primary threat: Coordinated TCP SYN scans from 5 distinct external IPs targeting the same internal host within seconds.
Risk Assessment
Critical Risks

Reconnaissance activity (Severity: High):
1,000 TCP SYN scans suggest attackers are mapping network defenses or identifying open ports.
Window size >1024 in SYN packets indicates potential use of **automated scanning tools** (e.g., Nmap with window size manipulation).
Secondary Risks

Concentrated targeting (Severity: Medium):
All malicious packets targeted 192.168.100.99, suggesting this host may be improperly exposed or prioritized by attackers.
Threat Observations
Technical Findings

Scan pattern:
SYN flag with abnormal window size (1024+), inconsistent with standard TCP handshake behavior.
Source IPs 63.2.154.223, 68.51.139.235, 136.237.33.61, 118.134.247.33, and 190.98.141.113 sequentially probed the target within 25 milliseconds (Packets #39-54).
Traffic context:
0 malicious TCP/UDP/ICMP/ARP packets detected outside of scan alerts.
No port-specific targeting observed (destination ports null in logs).
Statistical Highlights

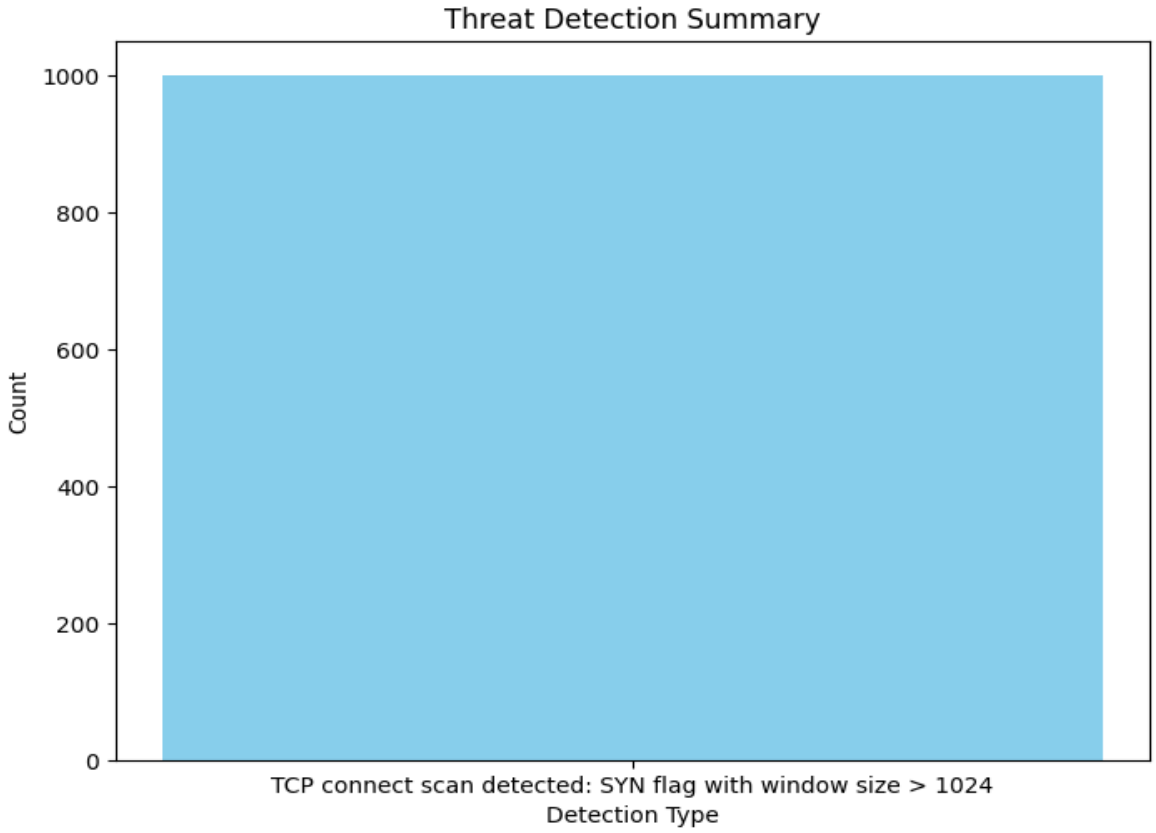
100% of alerts correlated to TCP connect scans.
5 attacker IPs generated 1,000 alerts, indicating **high-volume automated scanning**.
Recommendations
Immediate Actions

Block source IPs at the firewall:
Implement ACL rules to deny traffic from 63.2.154.223, 68.51.139.235, 136.237.33.61, 118.134.247.33, and 190.98.141.113.
Tune IDS/IPS thresholds:
Set alerts for SYN packets with window size >1024 when exceeding 10/minute per source IP.
Long-Term Mitigations

Segment network access:

Restrict inbound TCP connections to 192.168.100.99 unless explicitly required.
Deploy scan mitigation:
Enable SYN cookies on border routers/firewalls.
Configure rate limiting for SYN packets (max 5/sec per source IP).
Threat intelligence integration:
Cross-reference attacker IPs with abuse databases (e.g., AbuseIPDB) for pattern analysis.

Threat Detection Summary



Detection Type	Count
TCP connect scan detected: SYN flag with window size > 1024	1000