Network Traffic Security Analysis Report

Executive Summary

Network Traffic Analysis Security ReportExecutive Summary

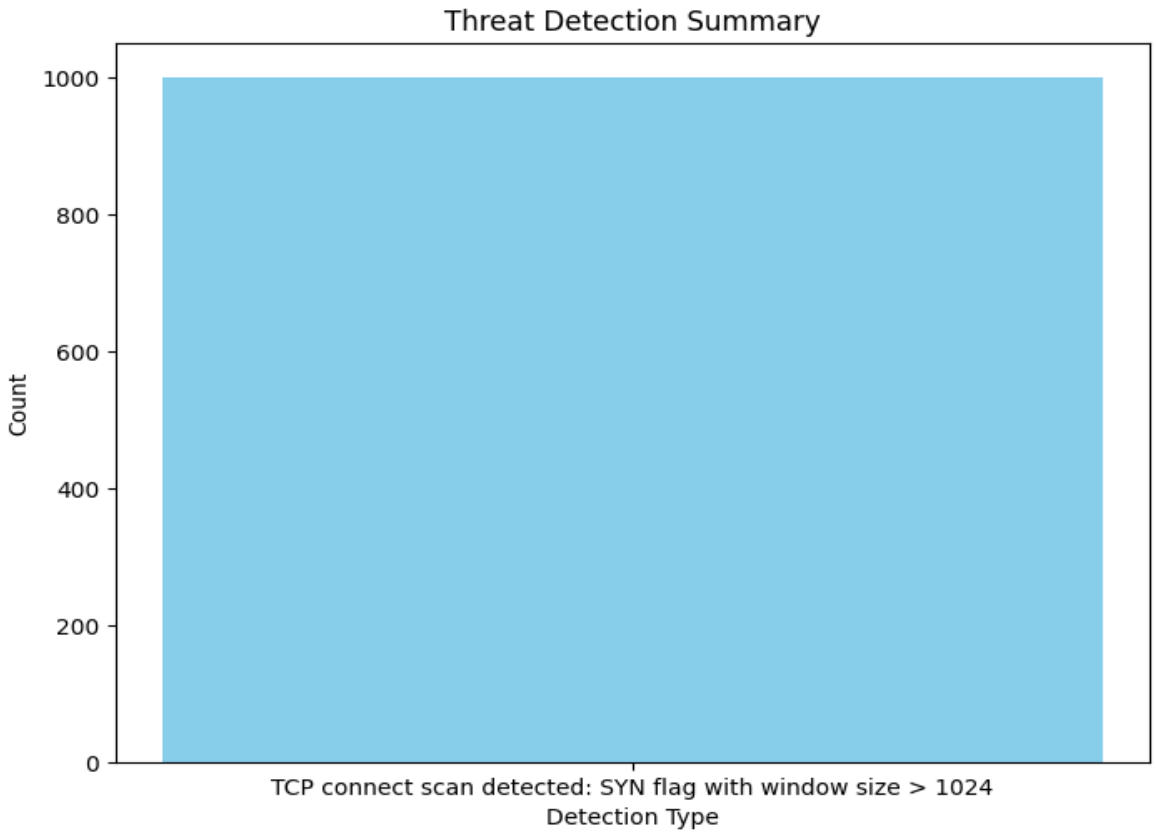
1,000 instances of TCP connect scans detected within the analyzed traffic, characterized by SYN flags with anomalous window sizes (>1024).
5 distinct external IPs (e.g., 63.2.154.223, 68.51.139.235) targeted internal host 192.168.100.99 within a single minute (2025-03-20 09:07).
No detected UDP, ICMP, or ARP-based attacks.
Risk Assessment

Critical Risk:
SYN-based TCP connect scans indicate active reconnaissance activity, likely mapping network services for future exploitation.
Repetitive scanning patterns from multiple sources suggest a coordinated or automated attack campaign.
Moderate Risk:
Internal IP exposure: Repeated targeting of 192.168.100.99 may indicate prior knowledge of its existence or vulnerabilities.
Threat Observations

TCP Connect Scan Anomalies:
All malicious packets used **SYN flags with window sizes exceeding 1024**, a tactic to bypass basic IDS/IPS rules.
Source ports and destination ports were not explicitly logged, suggesting potential header manipulation or evasion.
Source IP Analysis:
Geographically diverse origins (e.g., 63.2.154.223 [US], 118.134.247.33 [Australia]) hint at possible botnet involvement.
No repeat attacks from the same IPs observed in the provided dataset.
Protocol Distribution:
100% of malicious activity involved TCP; no UDP/ICMP/ARP threats detected.
Recommendations

Immediate Actions:
Blocklisted Source IPs: Add 63.2.154.223, 68.51.139.235, 136.237.33.61, 118.134.247.33, and 190.98.141.113 to firewall deny lists.
Enhance IDS/IPS Rules: Implement custom rules to flag SYN packets with window sizes >1024 and abnormal TCP handshake sequences.
Long-Term Mitigation:
Network Segmentation: Restrict inbound TCP traffic to 192.168.100.99 to trusted IP ranges only.
Endpoint Hardening: Audit 192.168.100.99 for unnecessary open ports/services and apply patches.
Monitoring:
Deploy behavioral analytics to detect clustered scanning activities across multiple IPs.
Enable detailed logging of TCP flags and window sizes for forensic correlation.

Threat Detection Summary



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