Network Traffic Security Analysis Report

Executive Summary

Network Traffic Analysis Security ReportExecutive Summary

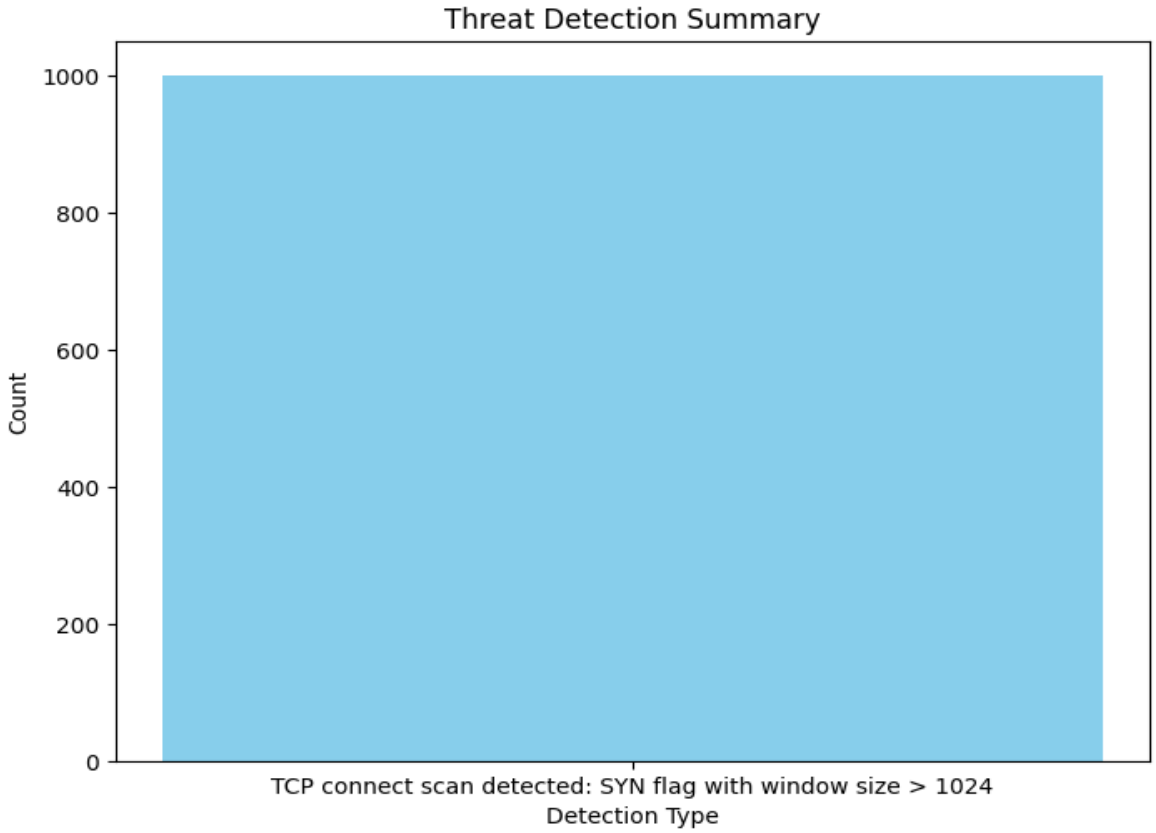
1,000 instances of TCP connect scans detected, all exhibiting SYN flags with window sizes > 1024.
Scans originated from **five distinct external IPs**, targeting internal host 192.168.100.99.
No malicious TCP/UDP/ICMP/ARP packets observed beyond reconnaissance activity.
Risk Assessment

High Risk: TCP connect scans indicate **active reconnaissance** by threat actors probing for vulnerabilities.
Impact: Potential precursor to exploitation (e.g., service enumeration, brute-force attacks).
Severity: Elevated due to volume (1,000 detections) and persistence across multiple sources.
Moderate Risk: Lack of port/destination details limits granular threat assessment.
Threat Observations

Scanning Technique:
All scans used **TCP SYN packets with abnormally large window sizes (>1024)**, a tactic to bypass basic IDS/IPS rules.
Source IPs (63.2.154.223, 68.51.139.235, 136.237.33.61, 118.134.247.33, 190.98.141.113) are geographically diverse, suggesting **distributed scanning** or botnet involvement.
Target:
Focused on internal IP 192.168.100.99—potentially a critical asset (e.g., server, database).
Timing:
All scans occurred within **seconds** (09:07:47), indicating automated tools (e.g., Nmap, Masscan).
Recommendations

Immediate Actions:
Block source IPs at the firewall/IDS level.
Review logs on 192.168.100.99 for follow-up exploitation attempts (e.g., failed logins, unusual service requests).
Long-Term Mitigations:
Deploy TCP anomaly detection rules to flag SYN packets with window sizes >1024.
Segment the network to restrict external access to critical hosts like 192.168.100.99.
Enable rate-limiting for SYN packets to throttle scan attempts.
Forensic Follow-Up:
Correlate scans with threat intelligence feeds to identify known malicious IPs.
Conduct vulnerability assessment on 192.168.100.99 to address potential exposure.

Threat Detection Summary



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