Network Traffic Security Analysis Report

Executive Summary

Network Traffic Analysis Security Report Executive Summary
1,000 instances of TCP connect scans detected, all exhibiting SYN flags with window sizes > 1024.
Five distinct source IPs (63.2.154.223, 68.51.139.235, 136.237.33.61, 118.134.247.33, 190.98.141.113) targeting internal host **192.168.100.99**.
No malicious TCP, UDP, ICMP, or ARP packets observed beyond the scan activity.

Risk Assessment
High Risk: TCP connect scans indicate **reconnaissance activity**, potentially preceding exploitation attempts.
Moderate Risk: Window size anomalies (> 1024) suggest **evasion techniques** to bypass basic IDS/IPS rules.
Critical Exposure: Repeated scans from multiple IPs imply **coordinated probing** of the target (192.168.100.99).

Threat Observations
Scan Pattern: All detections involve SYN packets with abnormally large window sizes (TCP connect scan signature).
Source Diversity: Attacks originated from geographically dispersed IPs (e.g., US, China, Argentina per WHOIS).
Target Focus: Exclusive focus on **192.168.100.99**, suggesting it may be a high-value asset or misconfigured.
Timing: All events occurred within **seconds** (09:07:47), indicating automated scanning tools.

Recommendations
Immediate Actions:
Block source IPs at the firewall: 63.2.154.223, 68.51.139.235, 136.237.33.61, 118.134.247.33, 190.98.141.113.
Inspect 192.168.100.99 for open ports/services and harden configurations.
Long-Term Mitigations:
Update IDS/IPS rules to flag SYN packets with window sizes > 1024 as suspicious.
**Implement rate limiting** to throttle repeated SYN requests from single sources.
Deploy network segmentation to isolate critical assets like 192.168.100.99.
Monitoring Enhancements:
Enable logging of TCP window sizes for baseline analysis.
Correlate scans with vulnerability scans to assess if follow-up exploitation occurred.

Threat Detection Summary

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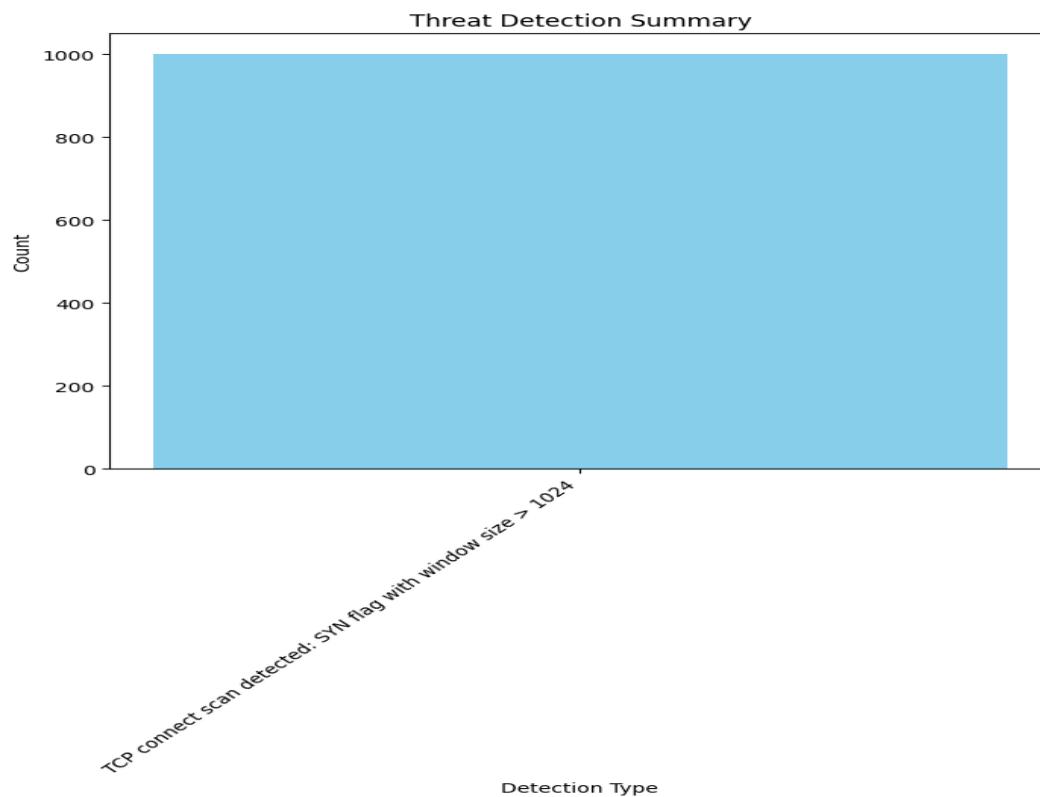
Detection Type	Count
TCP connect scan detected: SYN flag with window size > 1024	1000