

# Network Traffic Security Analysis Report

## Executive Summary

``markdown  
Executive Summary

**398 instances of TCP connect scans** detected originating from 192.100.100.100 targeting internal host 192.168.100.99.

**No other attack types observed** (TCP/UDP/ICMP/ARP packets associated with attacks: 0). Activity concentrated within a single minute (2025-03-20 13:42), indicating a rapid, targeted reconnaissance effort.

Risk Assessment

### Critical Risk:

**TCP SYN scan with anomalous window sizes (>1024)** – High-severity indicator of network enumeration. Attackers use oversized window sizes to evade legacy detection systems.

### High Risk:

**Focused targeting** – Repeated scans against 192.168.100.99 suggest deliberate reconnaissance for potential exploitation.

### Medium Risk:

**Lack of port visibility** – Missing source/destination port data limits granular threat analysis. Threat Observations

### Attack Pattern:

100% of top threats involve TCP SYN packets with window sizes exceeding 1024. Scans occurred at sub-second intervals (e.g., packets #1, #3, #5 within 0.12 seconds).

### Attacker Infrastructure:

Single source IP (192.100.100.100) with no observed port data, suggesting potential obfuscation.

### Target Profile:

All traffic directed to 192.168.100.99, likely a high-value internal asset.

### Recommendations

#### Immediate Actions:

**Block 192.100.100.100** at the network firewall and alert on future communication attempts. Update IDS/IPS rules to **flag SYN packets with window sizes >1024** as high-priority events.

#### Network Hardening:

Implement **SYN packet rate limiting** to throttle scan attempts.

**Segment 192.168.100.99** into a restricted VLAN to limit lateral movement.

#### Visibility Improvements:

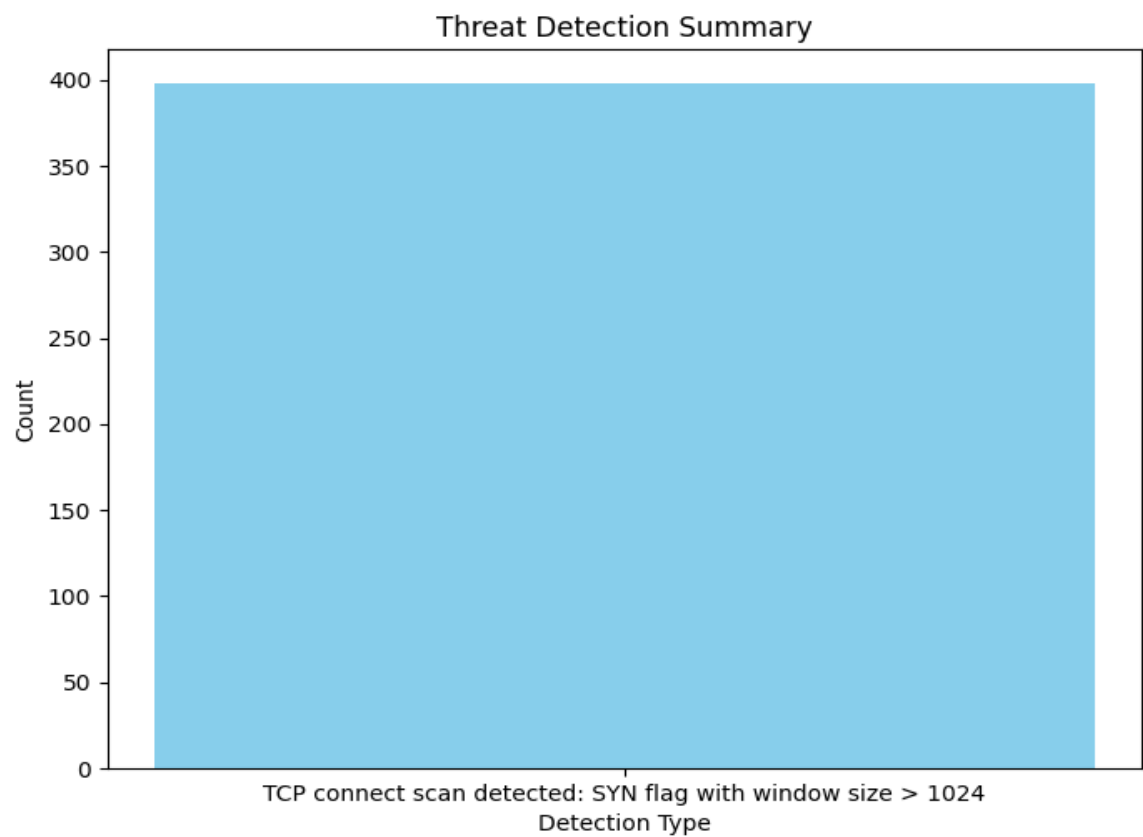
Enable full packet capture for traffic involving critical assets to **log source/destination ports**. Deploy endpoint monitoring on 192.168.100.99 to correlate network scans with host-level activity.

#### Proactive Measures:

Conduct a **vulnerability assessment** on 192.168.100.99 to address potential exploit pathways. Validate firewall rules to ensure unnecessary ports/services are not exposed to untrusted networks.

..

**Threat Detection Summary**



Detection Type	Count
TCP connect scan detected: SYN flag with window size > 1024	398