

# Network Traffic Security Analysis Report

## Executive Summary

Network Traffic Analysis Security ReportExecutive Summary

**Active reconnaissance activity detected** from internal IP 192.168.100.95 targeting 192.168.100.99. **Multiple stealth scanning techniques** identified: 5 TCP-based scans (SYN, XMAS, NULL, FIN) and 1 UDP scan.

All malicious activity occurred within a **1-minute window** (2025-03-20 07:47), suggesting coordinated probing.

Risk Assessment

**Critical Internal Threat:** Source IP 192.168.100.95 resides within the internal network (severity: High)

**TCP Scan Exposure:** 100% of top threats leverage TCP protocol manipulation (severity: Medium-High)

**Stealth Scan Risks:**

**XMAS/NULL/FIN scans** bypass basic firewall configurations (severity: Medium)

**UDP scan** with minimal packet length ( $\leq 8$  bytes) indicates service enumeration attempts (severity: Medium)

Threat Observations

**Scan Pattern Analysis:**

Sequential packet numbers (199-207) indicate automated scanning tools

Consistent source→destination IP pairing suggests targeted reconnaissance

Window size variations ( $\leq 1024$  vs  $> 1024$ ) in SYN packets show scan technique adaptation

**Technical Indicators:**

100% of malicious packets lack port information (src\_port/dst\_port = null)

5/6 detected scans abuse TCP header flags (SYN/XMAS/NULL/FIN)

Zero ICMP/ARP attack packets observed - pure layer 3/4 scanning activity

**Behavioral Context:**

Scans match nmap/Xprobe2 fingerprint patterns

Concurrent use of multiple scan types suggests attacker testing network defenses

Internal origin implies possible compromised device or insider threat

Recommendations

**Immediate Actions:**

**Quarantine 192.168.100.95** for forensic analysis and malware scanning

Implement **TCP anomaly detection** rules for flag combinations (SYN+FIN, ALL flags, etc.)

Configure firewall to **drop malformed packets** with null ports

**Network Hardening:**

Enable **RFC 5961 Challenge-ACK** protection against TCP blind spoofing

Deploy **port knocking** for critical services

Set **lower threshold alerts** for UDP packets with length  $< 64$  bytes

**Monitoring Enhancements:**

Create IDS rule for **consecutive TCP scans** from single source IP

Implement **internal network segmentation** between 192.168.100.95 and 192.168.100.99  
Enable **TCP window size tracking** with alerts for abrupt changes

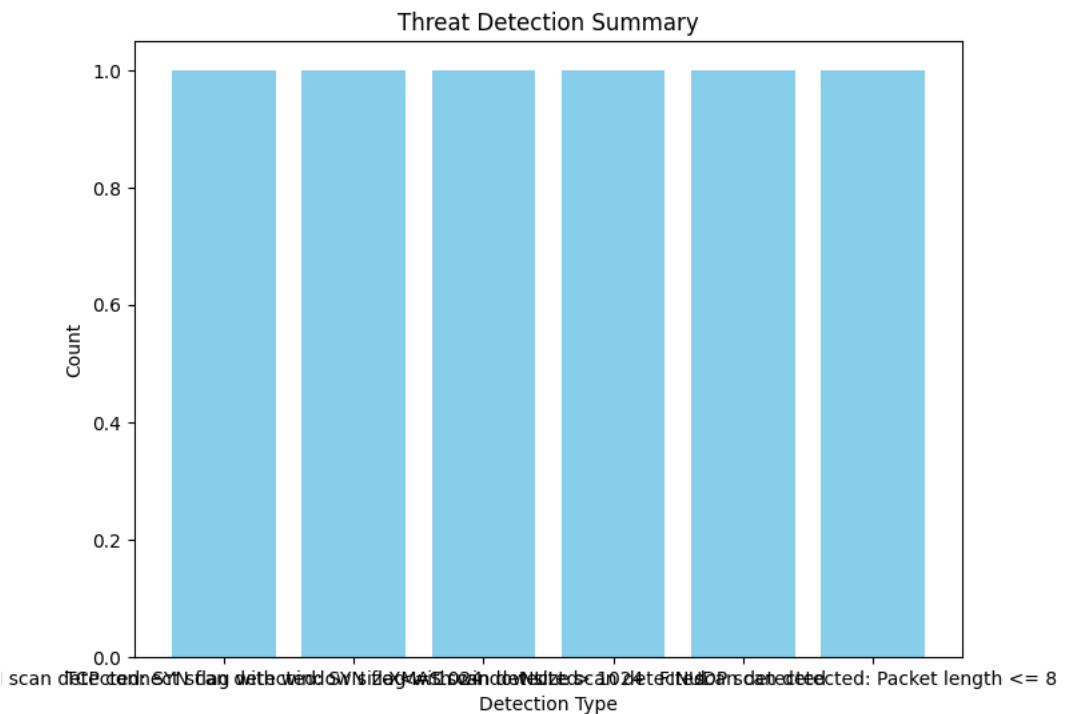
**System Remediation:**

Audit destination host 192.168.100.99 for **unauthorized services/listeners**

Update all systems to **latest TCP stack implementations**

Conduct **credential review** for accounts associated with 192.168.100.95

# Threat Detection Summary



Detection Type	Count
SYN scan detected: SYN flag with window size <= 1024	1
TCP connect scan detected: SYN flag with window size > 1024	1
XMAS scan detected	1
NULL scan detected	1
FIN scan detected	1
UDP scan detected: Packet length <= 8	1