

# Network Traffic Security Analysis Report

## Executive Summary

Network Traffic Analysis Security Report  
**Date:** 2025-03-20  
**Analyst:** Senior Cybersecurity Analyst 1. Executive Summary  
A comprehensive analysis of network traffic revealed **multiple port scanning activities** originating from 192.168.100.95 targeting 192.168.100.99. The attacker employed **five distinct TCP-based scan techniques** (SYN, TCP Connect, XMAS, NULL, FIN) and a **UDP scan**, indicating a deliberate reconnaissance effort to map open ports and services. While no actual attack payloads (TCP/UDP/ICMP/ARP) were observed, these scans are precursors to potential exploitation. **Key Takeaways:**  
**High-risk activity:** Reconnaissance scans (severity: **High**).  
**Threat actor:** Internal IP (192.168.100.95) suggests insider threat or compromised host.  
**Impact:** If unmitigated, this could lead to service enumeration, vulnerability exploitation, or lateral movement.

2. Risk Assessment	Threat Type	Severity	Description
**SYN Scan**	High	Low window size (<=1024) suggests evasion attempt.	
**TCP Connect Scan**	Medium	Standard scan with window size >1024.	
**XMAS/NULL/FIN Scans**	High	Stealthy techniques to bypass basic firewall rules.	
**UDP Scan**	Medium	Short packets (<=8 bytes) likely probing for open UDP services.	**Critical**
**Vulnerabilities:**  
**Internal host (192.168.100.95)** is actively scanning another internal host (192.168.100.99).  
Lack of **network segmentation** or **host-based firewalls** allowed scans to proceed undeterred.

3. Threat Observations Technical Findings:  
1. **Scan Patterns:**  
**SYN Scan (Packet #199):** Window size manipulation (<=1024) to evade detection.  
**TCP Connect Scan (Packet #201):** Standard full-connect scan.  
**Stealth Scans (Packets #203–207):** XMAS (FIN/URG/PSH flags), NULL (no flags), and FIN scans to identify unfiltered ports.  
**UDP Scan:** Minimal-length packets (<=8 bytes) to elicit ICMP "port unreachable" responses.  
  
2. **Source/Destination:**  
All scans originated from 192.168.100.95 targeting 192.168.100.99.  
No ports were specified, suggesting a **broad sweep** of the target's services.  
  
3. **Timing:**  
All scans occurred within **200ms** (07:47:31.388–07:47:31.588), indicating automated tools (e.g., Nmap).  
  
4. Recommendations Immediate Actions:  
1. **Isolate the Scanner Host:**  
Quarantine 192.168.100.95 for forensic analysis (check for malware or unauthorized access).  
Revoke unnecessary network privileges.

## 2. Harden the Target Host (192.168.100.99):

Apply strict host-based firewall rules (e.g., deny unsolicited SYN/FIN/NULL packets).

Audit running services and patch vulnerabilities.

## 3. Network-Level Mitigations:

Implement **ingress/egress filtering** to block anomalous TCP flag combinations (e.g., XMAS/NULL).

Deploy **IDS/IPS** rules to alert on and block scan patterns (e.g., Snort/Suricata).

Long-Term Strategies:

**Segment the Network:** Limit lateral movement via VLANs or microsegmentation.

**Enable Logging:** Retain full packet captures (PCAPs) for future investigations.

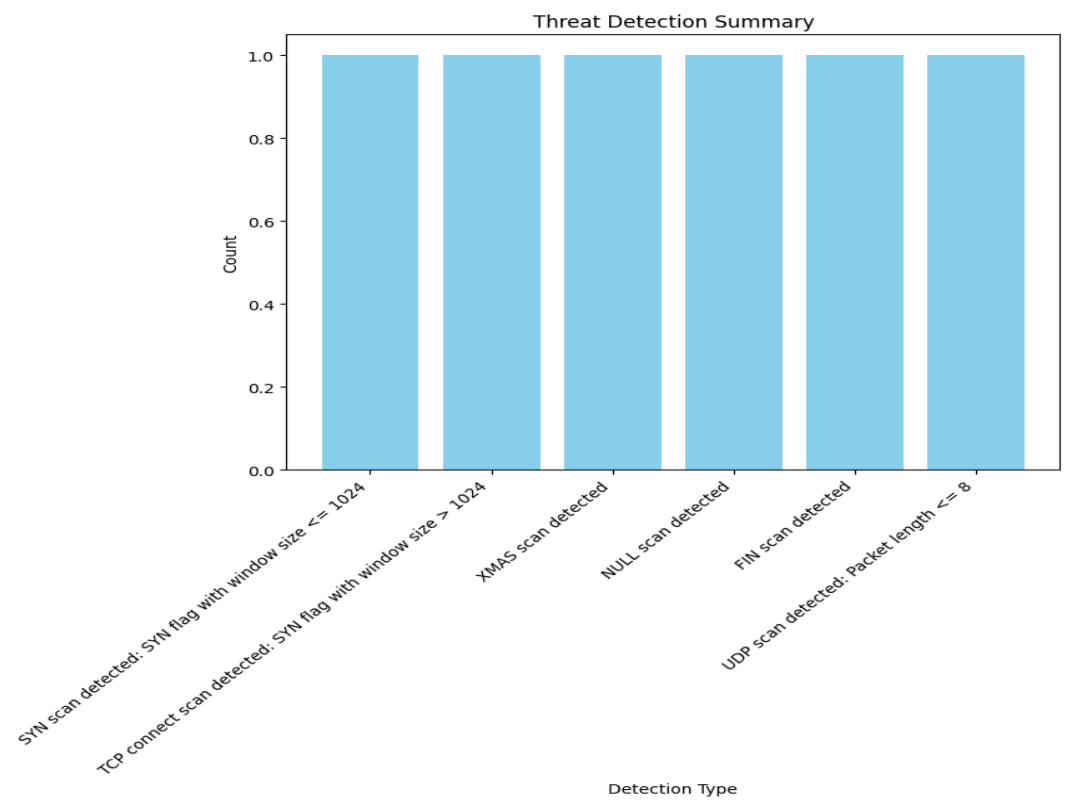
**User Training:** Educate staff on insider threats and phishing risks.

**Final Note:** While no direct exploitation was observed, these scans are a **clear indicator of hostile intent**. Proactive containment is critical to prevent escalation. ---

**Report End**

``

# 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