# Network Traffic Security Analysis Report

## *Overall Threat Assessment*

Threat Level: 6/10

## Executive Summary

Network Traffic Analysis Security ReportExecutive Summary

Multiple port scanning techniques detected from source IP 192.168.100.95 targeting 192.168.100.99.

**Critical reconnaissance activity** observed, including SYN, XMAS, NULL, FIN, and UDP scans.

All malicious traffic occurred within a single minute (2025-03-20 12:47), indicating a coordinated scan.

Risk Assessment

**High Risk**:

**SYN Scan (Window Size <= 1024)**: Indicates stealthy port scanning to identify open ports.

**XMAS/NULL/FIN Scans**: Evasion techniques to bypass basic firewall rules.

**Medium Risk**:

**TCP Connect Scan (Window Size > 1024)**: Less stealthy but still indicative of reconnaissance.

**UDP Scan (Packet Length <= 8)**: Probing for vulnerable UDP services.

Threat Observations

**Source IP 192.168.100.95** performed all malicious scans, suggesting an internal threat actor or compromised host.

**Scan Techniques Detected**:

SYN Scan (Packet #199, Window Size <= 1024)

TCP Connect Scan (Packet #201, Window Size > 1024)

XMAS Scan (Packet #203, Flags: FIN/URG/PSH)

NULL Scan (Packet #205, No Flags Set)

FIN Scan (Packet #207, FIN Flag Only)

UDP Scan (Short Packet Length)

**No actual attack packets (TCP/UDP/ICMP/ARP)** observed post-scan, indicating reconnaissance phase.

Recommendations

**Immediate Actions**:

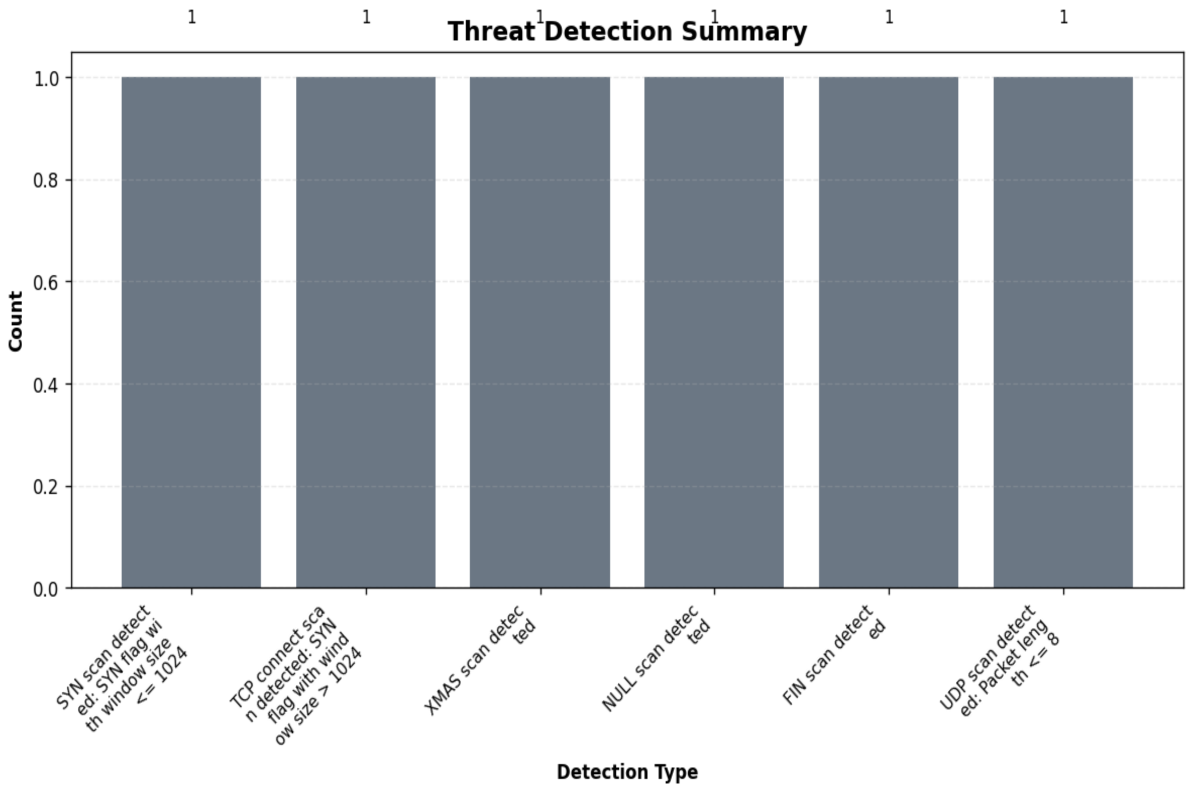
**Isolate 192.168.100.95** for forensic investigation to determine if it’s compromised.

**Block scanning IP** at the firewall level to prevent further reconnaissance.

**Long-Term Mitigations**:

**Enable Intrusion Prevention System (IPS)** to automatically drop scan attempts.
**Implement Network Segmentation** to restrict internal host communication.
**Update Firewall Rules** to reject malformed packets (e.g., NULL/XMAS/FIN scans).
**Conduct Endpoint Security Review** on 192.168.100.95 for malware or unauthorized tools.

# Threat Detection Summary



## *Detection Details*

| 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 |

## *Source/Destination Analysis*

| IP Address | As Source | As Destination | Total |
|---|---|---|---|
| 192.168.100.95 | 5 | 0 | 5 |
| 192.168.100.99 | 0 | 5 | 5 |

## *Event Timeline*

| Time | Packet # | Protocol | Detection |
|---|---|---|---|
| 12:47:31.388 | 199 | TCP | SYN scan detected: SYN flag wi<br/>th window size <= 1024 |
| 12:47:31.437 | 201 | TCP | TCP connect scan detected: SYN<br/> flag with window size > 1024 |
| 12:47:31.489 | 203 | TCP | XMAS scan detected |
| 12:47:31.541 | 205 | TCP | NULL scan detected |
| 12:47:31.588 | 207 | TCP | FIN scan detected |

# Appendix: Raw Traffic Analysis Data

```
{
  "detection_counts": {
    "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
  },
  "attack_stats": {
    "tcp_packets": 0,
    "udp_packets": 0,
    "icmp_packets": 0,
    "arp_packets": 0
  },
  "top_threats": [
    {
      "packet_number": 199,
      "timestamp": "2025-03-20T12:47:31.388726",
      "minute": "2025-03-20 12:47",
      "protocols": [
        "TCP"
      ],
      "src_ip": "192.168.100.95",
      "dst_ip": "192.168.100.99",
      "src_port": null,
      "dst_port": null,
      "detection_details": [
        "SYN scan detected: SYN flag with window size <= 1024"
      ]
    },
    {
      "packet_number": 201,
      "timestamp": "2025-03-20T12:47:31.437189",
      "minute": "2025-03-20 12:47",
      "protocols": [
        "TCP"
      ],
      "src_ip": "192.168.100.95",
      "dst_ip": "192.168.100.99",
      "src_port": null,
      "dst_port": null,
      "detection_details": [
        "TCP connect scan detected: SYN flag with window size > 1024"
      ]
    },
    {
      "packet_number": 203,
      "timestamp": "2025-03-20T12:47:31.489040",
      "minute": "2025-03-20 12:47",
      "protocols": [
        "TCP"
      ],
      "src_ip": "192.168.100.95",
      "dst_ip": "192.168.100.99",
      "src_port": null,
      "dst_port": null,
      "detection_details": [
        "XMAS scan detected"
      ]
    },
    {
      "packet_number": 205,
      "timestamp": "2025-03-20T12:47:31.541120",
      "minute": "2025-03-20 12:47",
      "protocols": [
        "TCP"
      ],
      "src_ip": "192.168.100.95",
      "dst_ip": "192.168.100.99",
      "src_port": null,
      "dst_port": null,
      "detection_details": [
        "NULL scan detected"
      ]
    },
    {
      "packet_number": 207,
      "timestamp": "2025-03-20T12:47:31.588889",
      "minute": "2025-03-20 12:47",
      "protocols": [
        "TCP"
      ],
      "src_ip": "192.168.100.95",
      "dst_ip": "192.168.100.99",
      "src_port": null,
      "dst_port": null,
      "detection_details": [
        "FIN scan detected"
      ]
    }
  ]
}
```

*This report was automatically generated by DeepSeek AI*
*Filename: security_report_20250425_104045.pdf*
*SHA-256 Hash: e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855*
*Generated on: 2025-04-25 10:41:11*