

# Network Traffic Security Analysis Report

## Overall Threat Assessment



## Executive Summary

Network Traffic Analysis Security ReportExecutive Summary

Multiple **port scanning activities** detected from source IP 192.168.100.95 targeting 192.168.100.99. Scans include **SYN, TCP connect, XMAS, NULL, FIN, and UDP scans**, indicating a **reconnaissance phase** of a potential attack. No malicious payloads observed in TCP/UDP/ICMP/ARP packets, but the scans suggest **probing for vulnerabilities**.  
Risk Assessment

### Critical Risk:

**Reconnaissance activity** (multiple scan types) from an internal IP (192.168.100.95), indicating a possible **compromised host or insider threat**.

### High Risk:

**XMAS, NULL, and FIN scans** are stealthy techniques to bypass basic firewall rules. **UDP scan** (packet length  $\leq 8$ ) suggests probing for open UDP services.

### Threat Observations

#### Scanning Techniques Detected:

- SYN scan** (window size  $\leq 1024$ ) – Packet #199.
- TCP connect scan** (window size  $> 1024$ ) – Packet #201.
- XMAS scan** (FIN/URG/PSH flags set) – Packet #203.
- NULL scan** (no flags set) – Packet #205.
- FIN scan** (only FIN flag set) – Packet #207.
- UDP scan** (short packets) – Indicates service enumeration.

**Source IP (192.168.100.95)** is internal, suggesting:

- A compromised device.
- Unauthorized internal scanning.

**Target IP (192.168.100.99)** may be a high-value asset.

### Recommendations

### **Immediate Actions:**

**Isolate 192.168.100.95** for forensic investigation.

**Review logs** on 192.168.100.99 for signs of exploitation.

### **Network Hardening:**

**Implement strict egress filtering** to block internal hosts from conducting scans.

**Enable TCP anomaly detection** (e.g., SYN flood protection, invalid flag combinations).

### **Monitoring Enhancements:**

**Deploy IDS/IPS rules** to detect and block stealth scans (XMAS/NULL/FIN).

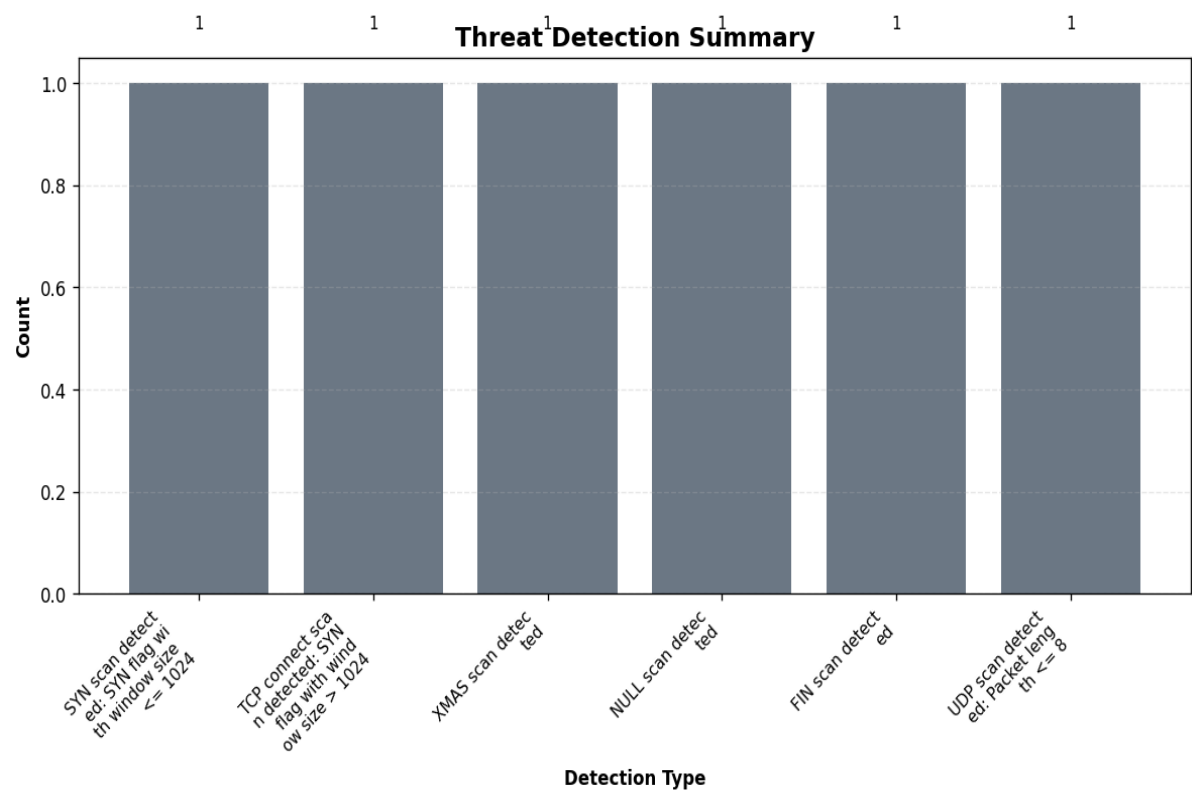
**Monitor UDP traffic** for unusual patterns (short packets, high frequency).

### **Policy Updates:**

**Restrict internal scanning** to authorized personnel only.

**Conduct a vulnerability assessment** on 192.168.100.99 to patch potential entry points.

# 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 with window size <= 1024
12:47:31.437	201	TCP	TCP connect scan detected: SYN 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\_104717.pdf*

*SHA-256 Hash: e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855*

*Generated on: 2025-04-25 10:47:49*