

# Network Traffic Security Analysis Report

## Overall Threat Assessment



## Executive Summary

Network Traffic Analysis Security ReportExecutive Summary

Multiple network reconnaissance activities detected from source IP 192.168.100.95 targeting 192.168.100.99.

**High-risk scanning techniques** observed, including SYN, XMAS, NULL, FIN, and UDP scans. No malicious payloads or successful exploitation attempts identified in the analyzed traffic.

### Critical Risk:

**Stealthy reconnaissance activity** (XMAS, NULL, FIN scans) indicates an attacker probing for vulnerabilities while evading basic detection.

**SYN scan with low window size** ( $\leq 1024$ ) suggests an attempt to identify open ports with minimal traffic.

### High Risk:

**TCP Connect Scan** (SYN flag with window size  $> 1024$ ) may indicate a more aggressive port scan. **UDP Scan** (Packet length  $\leq 8$ ) suggests an attempt to discover open UDP services.

### Threat Observations

### Scanning Techniques Detected:

- SYN Scan (Low Window Size):** Packet #199, likely probing for open ports stealthily.
- TCP Connect Scan (High Window Size):** Packet #201, indicative of a more direct scan.
- XMAS Scan:** Packet #203, using FIN, URG, PSH flags to bypass basic firewalls.
- NULL Scan:** Packet #205, sending a TCP packet with no flags to elicit responses from open ports.
- FIN Scan:** Packet #207, another evasion technique to identify open ports.
- UDP Scan:** Short-length packets ( $\leq 8$  bytes) suggest a UDP service discovery attempt.

### Source of Activity:

All malicious scans originated from 192.168.100.95 targeting 192.168.100.99. No ICMP or ARP-based attacks detected.

### Recommendations

### **Immediate Actions:**

**Block 192.168.100.95** at the firewall level to prevent further reconnaissance.

**Review logs** for prior activity from this IP to assess potential prior compromise.

### **Network Hardening:**

**Enable TCP SYN cookies** to mitigate SYN flood and scan attempts.

**Filter malformed TCP packets** (XMAS, NULL, FIN) at the firewall.

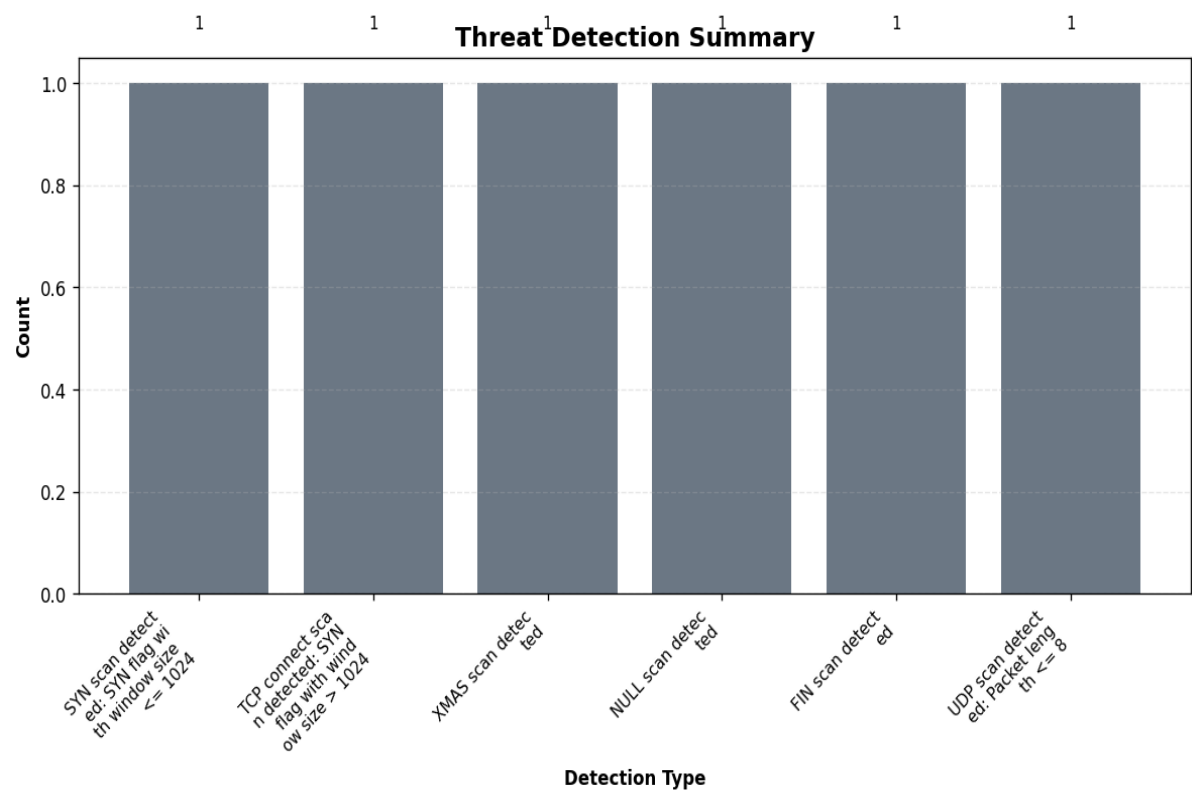
**Restrict UDP services** to only necessary ports and monitor for unusual traffic.

### **Detection Improvements:**

**Deploy an IDS/IPS** with rules to flag and block advanced scanning techniques.

**Implement rate limiting** on suspicious TCP/UDP traffic patterns.

# 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\_104542.pdf*

*SHA-256 Hash: e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855*

*Generated on: 2025-04-25 10:46:12*